

**FILED**

January 10, 2023

CLERK, U.S. DISTRICT COURT  
WESTERN DISTRICT OF TEXAS

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TEXAS  
WACO DIVISION**

BY: CV  
DEPUTY

TEXTILE COMPUTER SYSTEMS, INC.,

Plaintiff,

v.

REGIONS BANK, VISA INC., VISA  
U.S.A. INC., CAPITAL ONE, NATIONAL  
ASSOCIATION, JPMORGAN CHASE  
BANK, NATIONAL ASSOCIATION,  
AND CITIBANK, NATIONAL  
ASSOCIATION,

Defendants.

CIVIL ACTION NO. 6:22-cv-939-ADA

FIRST AMENDED COMPLAINT FOR  
PATENT INFRINGEMENT

**JURY TRIAL DEMANDED**

**FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT**

Plaintiff Textile Computer Systems, Inc. ("Textile" or "Plaintiff") files this first amended complaint against Defendants Regions Bank ("Regions"), Visa Inc., and Visa U.S.A. Inc. (together, "Visa"), Capital One, National Association ("Capital One"), JPMorgan Chase Bank, National Association ("Chase"), and Citibank, National Association ("Citibank") (collectively, "Defendants"), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

**PARTIES**

1. Textile Computer Systems, Inc. is a corporation formed under the laws of the State of Texas, with a place of business at 6517 Springwood Court, Temple, Texas, 76502.
2. Regions Bank is a Texas state bank with places of business in Austin.

3. Regions and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country's largest banking and financial service entities, including under the Regions brand.

4. Regions and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Regions and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Regions and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

7. Thus, Regions and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

8. Visa Inc. is a corporation organized and existing under the laws of Delaware. Visa Inc. may be served with process through its registered agent, The Corporation Trust Company, at Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801.

9. Visa U.S.A. Inc. is a corporation organized and existing under the laws of Delaware. Visa U.S.A. Inc. may be served with process through its registered agent, Corporation Service Company, at 211 E. 7th Street, Suite 620, Austin, Texas 78701.

10. Visa U.S.A. Inc. is a wholly-owned subsidiary of Visa Inc.

11. The Defendants identified in paragraphs 8-10 above (collectively, "Visa") and their affiliates lead and are part of an interrelated group of companies which together comprise

“one of the world’s leaders in digital payments” who “facilitate global commerce and money movement across more than 200 countries and territories among a global set of consumers, merchants, financial institutions and government entities through innovative technologies,”<sup>1</sup> including under the Visa brand.

12. The Visa defendants and their affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular. For example, Visa explains that “[u]nless the context indicates otherwise, reference to ‘Visa,’ ‘we,’ ‘us,’ ‘our’ or ‘the Company’ refers to Visa Inc. and its subsidiaries.”<sup>2</sup>

13. The Visa defendants and their affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

14. The Visa defendants and their affiliates regularly contract with customers and other financial institutions, payment networks, and processors regarding equipment or services that will be provided by their affiliates on their behalf.

15. Thus, the Visa defendants and their affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

16. Capital One, National Association is a national bank with a place of business in Austin, Texas. Capital One, National Association may be served with process through its

---

<sup>1</sup> See Visa, Inc.’s Form 10-K Annual Report, at 4 (Nov. 16, 2022). Available at <https://investor.visa.com/SEC-Filings/default.aspx#annual-filings>

<sup>2</sup> *Id.* at 2.

registered agent, Corporation Service Company, at 3366 Riverside Drive, Suite 103, Upper Arlington, Ohio 43221.

17. Capital One and its affiliates lead and are part of an interrelated group of companies which together comprise one of the world's largest credit card issuers, including under the Capital One brand.

18. Capital One and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

19. Capital One and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

20. Capital One and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

21. Thus, Capital One and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

22. JPMorgan Chase Bank, National Association is a national bank with places of business in Waco, Austin, San Antonio, and El Paso, Texas. JPMorgan Chase Bank may be served with process through its registered agent, CT Corporation System, at 4400 Easton Commons Way, Suite 125, Columbus, Ohio 43219.

23. Chase and its affiliates lead and are part of an interrelated group of companies which together comprise one of the world's largest credit card issuers, including under the Chase brand.



24. Chase and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

25. Chase and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

26. Chase and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

27. Thus, Chase and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

28. Citibank, National Association is a national bank with a place of business in San Antonio, Texas. Citibank, National Association may be served with process through its registered agent, CT Corporation System, at 4400 Easton Commons Way, Suite 125, Columbus, Ohio 43219.

29. Citibank and its affiliates lead and are part of an interrelated group of companies which together comprise one of the world's largest credit card issuers, including under the Citi and Citibank brands.

30. Citibank and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

31. Citibank and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

32. Citibank and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

33. Thus, Citibank and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

34. The parties to this action are properly joined under 35 U.S.C. § 299 because at least a portion of the right to relief asserted against Defendants jointly and severally arises out of the same series of transactions or occurrences relating to the making and using of the same accused instrumentalities, including authentication systems implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant that are provided, used, and/or made by Defendants. Additionally, questions of fact common to all defendants will arise in this action.

#### **JURISDICTION AND VENUE**

35. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

36. This Court has personal jurisdiction over Regions pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Regions has done and continues to do business in Texas; and (ii) Regions has committed and continues to commit acts of patent

infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

37. Venue is proper in this district as to Regions Bank pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Regions has committed and continues to commit acts of patent infringement in this district. For example, Regions cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make and/or use the accused instrumentalities in the district. Regions induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Regions has regular and established places of business in this district, including at least at 11215 Interstate 35, Suite 100, Austin, Texas 78747:





Locations Log In Open an Account En Español

Personal Small Business Commercial Wealth Insights

Help & Support Search



Full Service Bank Branch Open

## Shoppes At Onion Creek

### Lobby Hours

Mon - Fri: 9 a.m.-5 p.m.  
Sat: 9 a.m.-1 p.m.  
Sun: Closed

### Drive-Thru Hours

Mon - Fri: 9 a.m.-5 p.m.  
Sat: 9 a.m.-1 p.m.  
Sun: Closed

### Location

11215 Interstate 35, Suite 100  
Austin, TX 78747

### Contact

Make an Appointment 737-931-0100

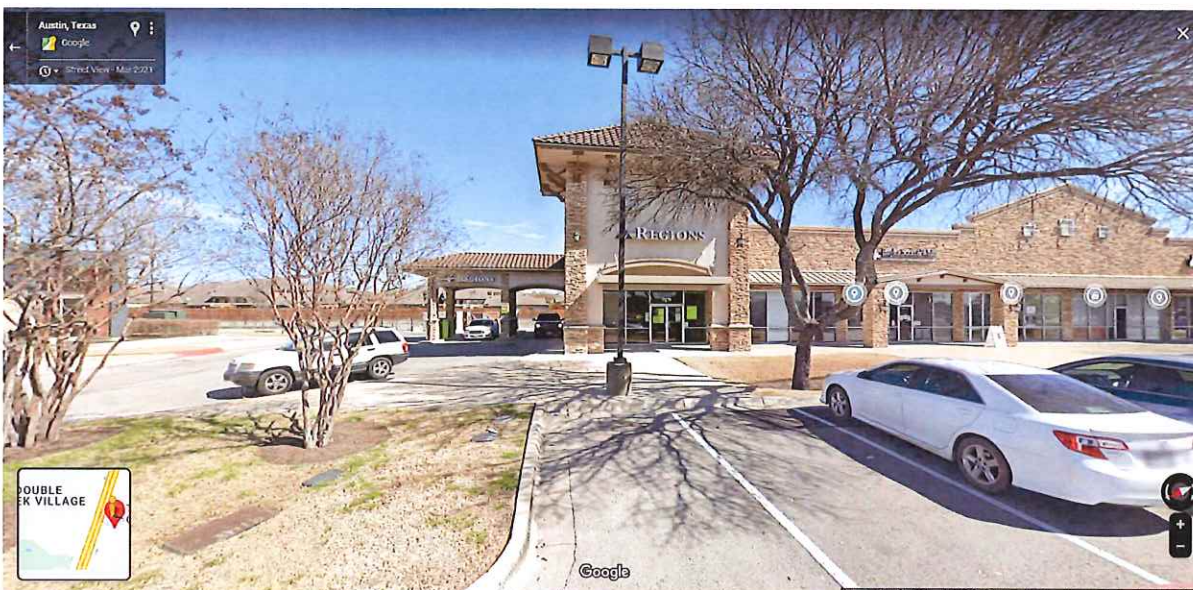
### Location Services

Make an Appointment



Feedback

(Source: <https://www.regions.com/locator/branch/bank-branch-shoppes-at-onion-creek-austin>)



(Source: screenshot from Google Maps Street View)





TRAVIS CENTRAL APPRAISAL DISTRICT  
TRAVIS COUNTY, TEXAS

## Property Search

Compound Text Search

regions bank

2022



Owner Name	Property Address	City	Legal Description	Market Value	Appraised Value
POWELL JACK J FAMILY TRUST	106 S TUMBLEWEED TRL		LOT 16 BLK A WOODLAKE TRAILS	\$1,285,139	\$1,285,139
REGIONS BANK	1721 WELLS BRANCH PKWY	AUSTIN	PERSONAL PROPERTY COMMERCIAL REGIONS BANK	\$131,447	\$131,447
REGIONS BANK	4314 W BRAKER LN	AUSTIN	PERSONAL PROPERTY COMMERCIAL REGIONS BANK	\$89,307	\$89,307
REGIONS BANK	6611 S MOPAC EXPRESSWAY		PERSONAL PROPERTY COMMERCIAL REGIONS BANK	\$104,990	\$104,990
REGIONS BANK	11215 S INTERSTATE HY 35	AUSTIN	PERSONAL PROPERTY COMMERCIAL REGIONS BANK	\$111,911	\$111,911
REGIONS BANK	6611 C S MOPAC EXPRESSWAY		LOT 2 GARZA/MCCOMIS SUBD AMD PLAT OF	\$1,800,000	\$1,800,000
REGIONS BANK	100 CONGRESS AVE	AUSTIN	PERSONAL PROPERTY COMMERCIAL REGIONS BANK	\$218,469	\$218,469

1

20

Per Page

(Source: screenshot from Travis County Appraisal District website)

38. This Court has personal jurisdiction over Visa pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Visa has done and continues to do business in Texas; (ii) Visa has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via offices, other locations, and branches of its customers, inducing others to commit acts of patent infringement in Texas, and/or committing at least a portion of any other infringements alleged herein; and (iii) Visa U.S.A. Inc. is registered to do business in Texas.

39. Venue is proper in this district as to Visa pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Visa has committed and continues to commit acts of patent infringement in this district. For example, Visa's customers' cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make and/or use the accused instrumentalities in the district. Visa induces others to commit acts of patent infringement in Texas, and/or commit at least a portion

of any other infringements alleged herein in this district. Visa has regular and established places of business in this district, including at least at 12301 Research Blvd, Austin, Texas 78759:



(Source: Screenshot from Google Maps Street View)



(Source: Screenshot from Google Maps Street View)

## Property Search

Compound Text Search  2022

Type	GEO ID	Owner Name	Property Address	City	Legal Description	Market Value	Appraised Value
P		VISA USA INC	12301 RESEARCH BLVD		PERSONAL PROPERTY COMMERCIAL VISA	\$11,624,021	\$11,624,021
P		VISA USA INC	12401 RESEARCH BLVD	AUSTIN	PERSONAL PROPERTY COMMERCIAL VISA	\$1,100,448	\$1,100,448

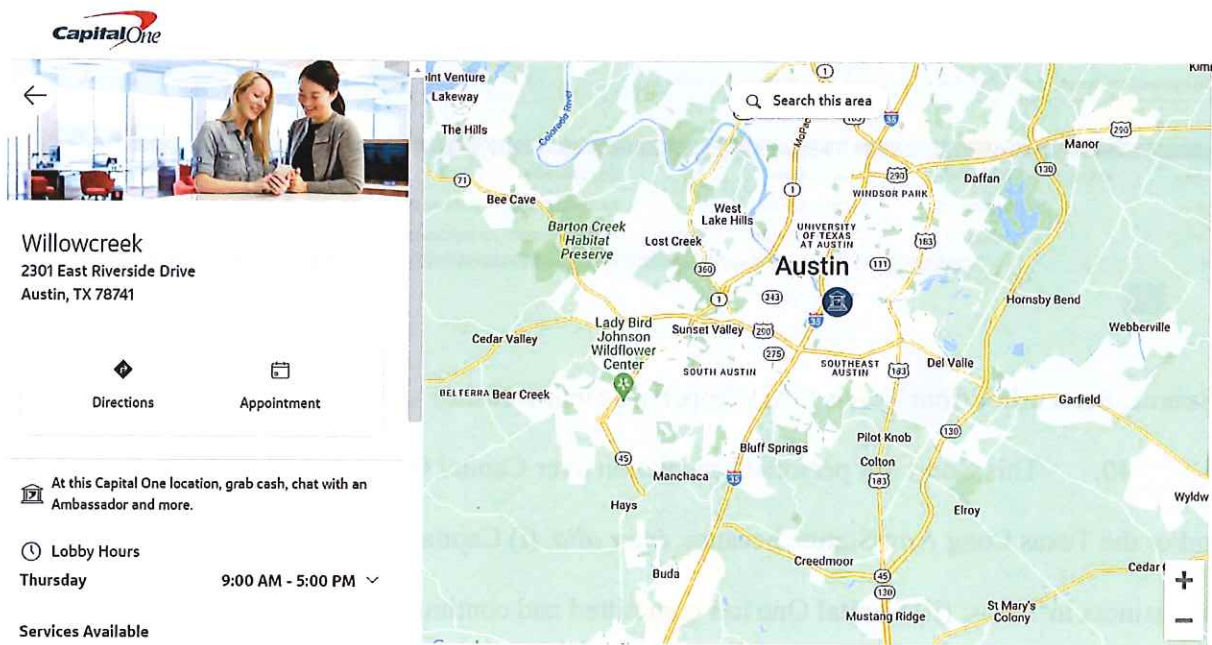
< 1 > 20 Per Page

(Source: Screenshot from Travis CAD Property Search website)

40. This Court has personal jurisdiction over Capital One pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Capital One has done and continues to do business in Texas; (ii) Capital One has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing at least a portion of any other infringements alleged herein; and (iii) Capital One is registered to do business in Texas.

41. Venue is proper in this district as to Capital One pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Capital One has committed and continues to commit acts of patent infringement in this district. For example, Capital One cardholders are issued Visa-branded debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make and/or use the accused instrumentalities in the district. Capital One induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Capital One has regular and established places of business in this district, including at least at 2301 East Riverside Drive, Austin, Texas 78741:





(Source: <https://locations.capitalone.com/bank/tx/Austin-Willowcreek-branch-41875?map=30.209484628797668,-97.7382491796875,12z&locTypes=branch&place=Austin,%20TX,%20USA&servicesFilter=>)



(Source: screenshot from Google Maps Street View)





TRAVIS CENTRAL APPRAISAL DISTRICT  
TRAVIS COUNTY, TEXAS

## Property Search

Compound Text Search  2022

Type	GEO ID	Owner Name	Property Address	City	Legal Description	Market Value	Appraised Value
P		CAPITAL ONE NA	4301 W WILLIAM CANNON DR	AUSTIN	PERSONAL PROPERTY COMMERCIAL CAPITAL ONE BANK	\$369,676	\$369,676
P		CAPITAL ONE NA	2301 E RIVERSIDE DR	AUSTIN	PERSONAL PROPERTY COMMERCIAL CAPITAL ONE BANK	\$183,073	\$183,073
P		CAPITAL ONE NA	11801 DOMAIN BLVD	AUSTIN	PERSONAL PROPERTY COMMERCIAL CAPITAL ONE CAFE	\$1,012,602	\$1,012,602
P		CAPITAL ONE NA	106 E 6 ST		PERSONAL PROPERTY COMMERCIAL CAPITAL ONE CAFE	\$659,111	\$659,111
P		CAPITAL ONE NA	3711 S MORAC EXPRESSWAY	AUSTIN	PERSONAL PROPERTY COMMERCIAL CAPITAL ONE NA	\$152,101	\$152,101
P		CAPITAL ONE NA	901 S MORAC EXPRESSWAY	AUSTIN	PERSONAL PROPERTY COMMERCIAL CAPITAL ONE NA	\$175,450	\$175,450
P		CAPITAL ONE NA	6317 BEE CAVE RD		PERSONAL PROPERTY COMMERCIAL CAPITAL ONE NA	\$50,621	\$50,621
P		CAPITAL ONE NA	301 W SLAUGHTER LN		PERSONAL PROPERTY COMMERCIAL CAPITAL ONE NA	\$87,109	\$87,109
P		CAPITAL ONE NA	4200 W BRAKER LLI		PERSONAL PROPERTY COMMERCIAL CAPITAL ONE NA	\$65,555	\$65,555
P		CAPITAL ONE NA	1400 SMITH RD	AUSTIN	PERSONAL PROPERTY COMMERCIAL CAPITAL ONE NA	\$10,381	\$10,381

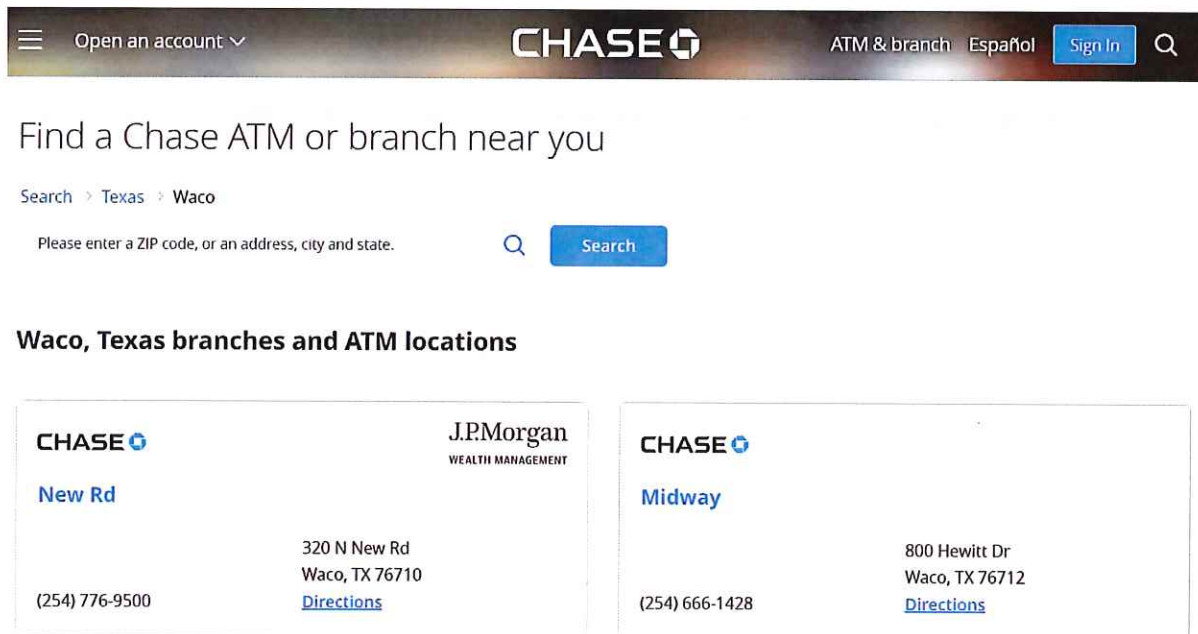
1 20 Per Page

(Source: screenshot from Travis CAD Property Search website)

42. This Court has personal jurisdiction over Chase pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Chase has done and continues to do business in Texas; (ii) Chase has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing at least a portion of any other infringements alleged herein; and (iii) Chase is registered to do business in Texas.

43. Venue is proper in this district as to Chase pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Chase has committed and continues to commit acts of patent infringement in this district. For example, Chase cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make and/or use the accused instrumentalities in the district. Chase induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Chase has regular and established places of business

in this district, including at least at 320 N New Road, Waco, TX 76710, at 800 Hewitt Drive, Waco, TX 76712, and at multiple branch locations in Austin, San Antonio, and El Paso:



(Source: <https://locator.chase.com/tx/waco>)



(Source: screenshot from Google Maps Street View)





(Source: screenshot from Google Maps Street View)

**McLennan CAD** Property Search Map Search

**Property Search Results > 1 - 3 of 3 for Year 2022** [Export Results](#) [New Search](#)

*Click the "Details" or "Map" link to view more information about the property or click the checkbox next to each property and click "View Selected on Map" to view the properties on a single map.*

○ Property Address ● Legal Description

	Property ID	Geographic ID	Type	Property Address	Owner Name	DBA Name	Appraised Value	
<input type="checkbox"/>	335742	362660000024060	Real	800 HEWITT DR WOODWAY, TX 76712	JPMORGAN CHASE BANK NA	CHASE BANK	\$1,560,870	<a href="#">View Details</a> <a href="#">View Map</a>
<input type="checkbox"/>	341699	48J113750	Personal	320 N NEW ROAD TX	JPMORGAN CHASE BANK NA	JPMORGAN CHASE BANK NA	\$264,680	<a href="#">View Details</a>
<input type="checkbox"/>	336762	36J113010	Personal	800 HEWITT DR TX	JPMORGAN CHASE BANK NA	JPMORGAN CHASE BANK NA	\$61,940	<a href="#">View Details</a>

Page: 1

**Questions Please Call (254) 752-9864**

Website version: 1.2.2.33 Database last updated on: 12/7/2022 10:40 PM © N. Harris Computer Corporation

(Source: screenshot from McLennan CAD Property Search website)

 Open an account ▾
 
 ATM & branch Español Sign In 





### Austin, Texas branches and ATM locations

<b>CHASE</b>  <b>Plaza Saltillo</b>  1011 E 5th St Ste 100 Austin, TX 78702 (737) 220-9674 <a href="#">Directions</a>	<b>J.P.Morgan</b> WEALTH MANAGEMENT  <b>CHASE</b>  <b>Plaza Volente</b>  11521 N FM 620 Rd Ste D Austin, TX 78726 (512) 506-3000 <a href="#">Directions</a>
<b>CHASE</b>  <b>Domain</b>  11800 Domain Dr Austin, TX 78758 (512) 719-5554 <a href="#">Directions</a>	<b>J.P.Morgan</b> WEALTH MANAGEMENT  <b>CHASE</b>  <b>Research</b>  12222 Research Blvd Austin, TX 78759 (512) 219-4400 <a href="#">Directions</a>

(Source: <https://locator.chase.com/tx/austin>)




 Open an account ▾
 
 ATM & branch Español Sign In 

### San Antonio, Texas branches and ATM locations

<b>CHASE</b>  <b>Basse and Nacogdoches</b>  1000 E Basse Rd San Antonio, TX 78209 (210) 829-6152 <a href="#">Directions</a>	<b>J.P.Morgan</b> WEALTH MANAGEMENT  <b>CHASE</b>  <b>Culebra</b>  10680 Culebra Rd San Antonio, TX 78251 (210) 647-2900 <a href="#">Directions</a>
<b>CHASE</b>  <b>Potranco and Rousseau</b>  10810 Potranco Rd San Antonio, TX 78251 (210) 520-5807 <a href="#">Directions</a>	<b>CHASE</b>  <b>Goliad</b>  1100 Goliad Rd San Antonio, TX 78223 (210) 534-8310 <a href="#">Directions</a>

(Source: <https://locator.chase.com/tx/san-antonio>)




[Open an account](#)

[ATM & branch](#)
[Español](#)
[Sign In](#)


### El Paso, Texas branches and ATM locations

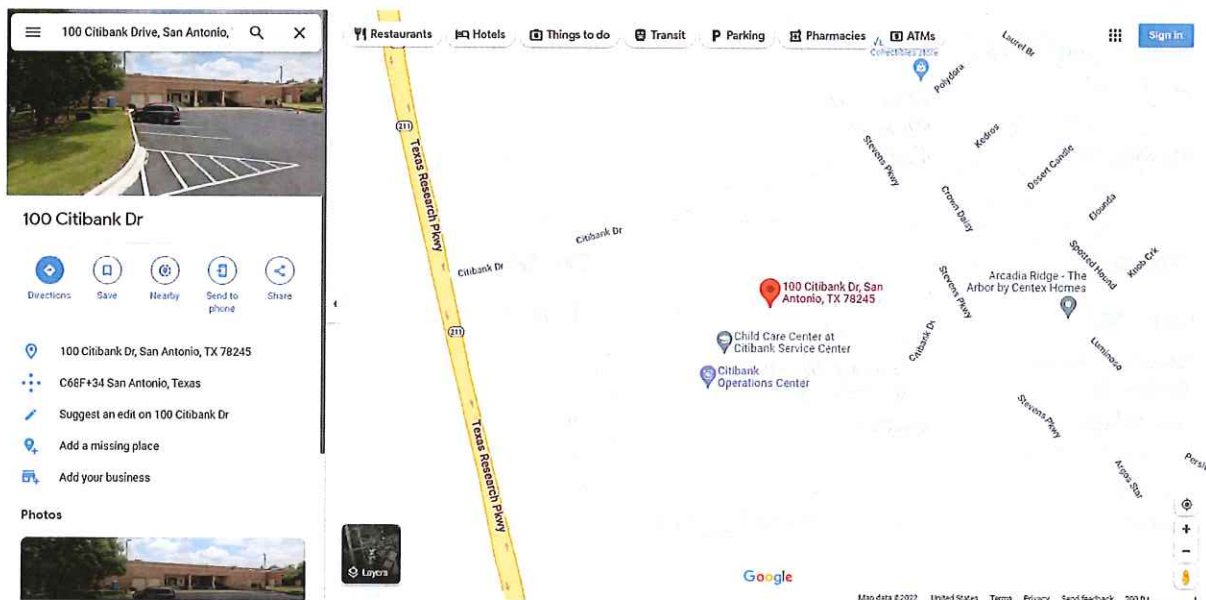
<b>CHASE</b> <b>Montana and Loop 375</b>  12244 Montana Ave El Paso, TX 79938 (915) 856-3827 <a href="#">Directions</a>	<b>CHASE</b> <b>Coronado</b>  135 Shadow Mountain Dr El Paso, TX 79912 (915) 585-4012 <a href="#">Directions</a>
<b>CHASE</b> <b>Park East</b>  ATM Only/No Branch ATM Open 24 Hours (800) 935-9935 1475 George Dieter Dr El Paso, TX 79936 <a href="#">Directions</a>	<b>CHASE</b> <b>El Paso East</b>  1533 N Lee Trevino Dr El Paso, TX 79936 (915) 594-4169 <a href="#">Directions</a>

(Source: <https://locator.chase.com/tx/el-paso>)

44. This Court has personal jurisdiction over Citibank pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Citibank has done and continues to do business in Texas; (ii) Citibank has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via offices and other locations, inducing others to commit acts of patent infringement in Texas, and/or committing at least a portion of any other infringements alleged herein; and (iii) Citibank is registered to do business in Texas.

45. Venue is proper in this district as to Citibank pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Citibank has committed and continues to commit acts of patent infringement in this district. For example, Citibank cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make and/or use the accused instrumentalities in the district. Citibank induces

others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Citibank has regular and established places of business in this district, including at least at 100 Citibank Drive, San Antonio, Texas 78245:



(Source: screenshot from Google Maps)



(Source: screenshot from Google Maps Street View)

# Client Manual – Consumer Accounts

---

## U.S. Markets

Effective November 18, 2021

Welcome to Citibank and thank you for choosing us for your banking needs.

This manual contains some important information you should know about your deposit relationship with Citibank. It is an agreement between you and us. From Account Transactions to Electronic Banking and beyond, we want you to understand how our products and services work, as well as to understand some of the important responsibilities that exist – yours and ours.

\*\*\*

### Rules for Rejecting This Arbitration Provision

You may reject this arbitration provision by sending a written rejection notice to us at: 100 Citibank Drive, Attn: Arbitration Opt Out, San Antonio, TX 78245. Your rejection notice must be mailed within 45 days of account opening. Your rejection notice must state that you reject the arbitration provision and include your

(Source: screenshots of PDF available at:

[https://online.citi.com/JRS/popups/ao/Consumer\\_Client\\_Manual.pdf](https://online.citi.com/JRS/popups/ao/Consumer_Client_Manual.pdf))

### **BACKGROUND**

46. The patents-in-suit generally pertain to payment authorization technology used in payment networks used to process transactions from, for example, credit cards and debit cards. The technology disclosed by the patents was developed by Gopal Nandakumar, a Texas-based entrepreneur, software engineer, and prolific inventor with over 30 years of experience in the field of Information Management Systems.



47. In 1987, after receiving Master's Degrees from both the University of Madras, India and the Georgia Institute of Technology, Mr. Nandakumar formed Textile Computer Systems, Inc. ("Textile") for the purpose of consulting and developing software for the textile industry. In 2005, Textile began transitioning into credit card transaction systems. In 2011, Textile began to develop and market the MySingleLink suite of applications.

48. The Nandakumar patents are related to payment authorization technology. Mr. Nandakumar has been at the forefront of payment authorization, developing, disclosing, and patenting solutions for reducing fraud in credit and debit card transactions. Indeed, the Nandakumar patents (or the applications leading to them) have been cited during patent prosecution over a hundred times, including by numerous leading companies in the payment authorization industry such as ADP, Bank of America, Google, Groupon, IBM, Mastercard, NEC, Paypal, and Wells Fargo.

### **THE TECHNOLOGY**

49. The patents-in-suit, U.S. Patent Nos. 8,505,079, 8,533,802, 10,148,659, and 10,560,454 (collectively, the "Asserted Patents"), teach systems, including payment processing systems, for securely and effectively approving and processing specific credit card and/or debit card transactions. Through the specific use of servers, messaging gateways, and/or interfaces, these systems act to reduce credit card and/or debit card fraud and misuse through their use and validation of key strings, authentication credentials, transaction specific information, and transaction specific credentials. The technology in the Asserted Patents improves the underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.



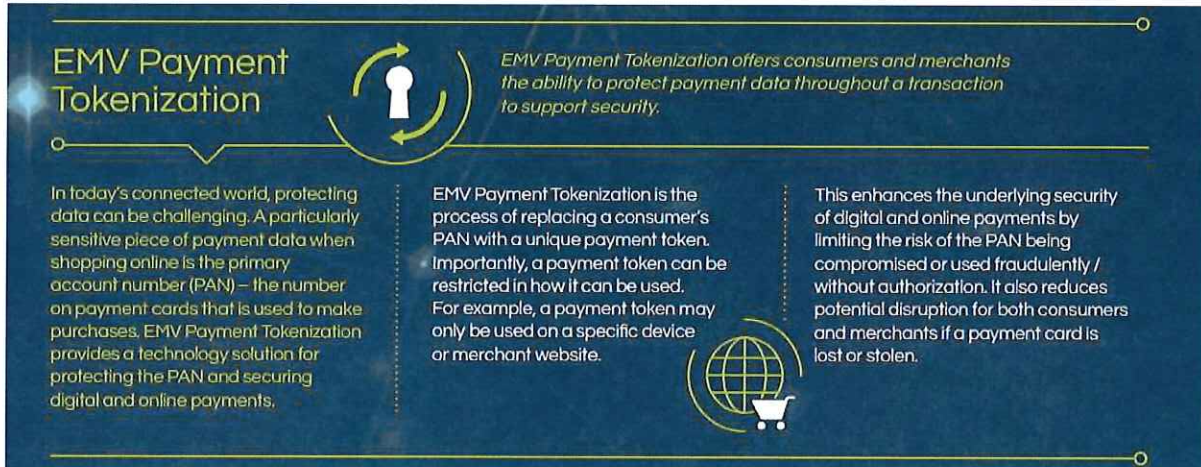
50. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have led to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall's, was hit with a cyber attack that resulted in the theft of credit cards leading to over \$100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

51. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as "a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment" and as "enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs."

(Source: <https://www.emvco.com/emv-technologies/payment-tokenisation/>).

52. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a number of years to develop infringing payment tokenisation systems. In other words, the technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

53. Indeed, as recently as February of 2021, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents "provides a technology solution for protecting the PAN and securing digital and online payments":



(Source: [https://www.emvco.com/wp-content/uploads/documents/Quick-Resource\\_How-EMV-Specifications-Support-Online-Commerce.pdf](https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf))

54. That same EMVCo document notes that “In today’s connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases” and that EMVCo’s payment tokenization “enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization.” The document also states that the “Payment Tokenisation Specification provides an interoperable Technical Framework.” (Source: [https://www.emvco.com/wp-content/uploads/documents/Quick-Resource\\_How-EMV-Specifications-Support-Online-Commerce.pdf](https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf))

55. One of the asserted patents, the 079 Patent, was challenged in an Inter Partes Review proceeding before the Patent and Trademark Office (“PTO”). The PTO found that the challenger, Unified Patents Inc., was unable to show that one element, the “key string” as claimed in the 079 Patent claims and as construed by the PTO, was in the prior art at all, much

less it being conventional or widespread. The PTO thus confirmed the patentability of all challenged claims of the 079 Patent.

**COUNT I**

**INFRINGEMENT OF U.S. PATENT NO. 8,505,079**

56. On August 6, 2013, United States Patent No. 8,505,079 (“the 079 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

57. Textile is the owner of the 079 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 079 Patent against infringers, and to collect damages for all relevant times.

58. Regions, Capital One, Chase, and Citibank offer Visa-branded debit and/or credit cards, such as the Regions Visa Debit Card, various Regions Visa Credit Cards, the Capital One Venture X Visa Credit Card, the Capital One Venture Visa Credit Card, the Capital One Journey Visa Credit Card, the Chase Freedom Unlimited Visa Credit Card, the Chase Sapphire Preferred Visa Credit Card, the Chase Sapphire Reserve Visa Credit Card, the Citibank Costco Anywhere Visa Credit Card, and the Citibank Costco Anywhere Visa Business Credit Card, that are used with Regions, Capital One, Chase, and/or Citibank authentication systems that authenticate the identity of a Regions, Capital One, Chase, or Citibank card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). Visa provides tokenization and processing services to banks for the purposes of using the Accused Instrumentality card authentication system. The Accused Instrumentality card authentication systems that are used, made, and sold by Regions, Capital One, Chase, Citibank, and Visa are implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card



number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities, for example. The requests are initiated by account holders via their smartphones or computers and use those tokens, which are generated and communicated by the system, and wherein each account held by the user has its own token.


## Click to Pay with Visa

*Transfer Money and Pay*




Click to Pay with Visa<sup>1</sup> is the easy, smart and secure way to shop online with your smartphone, tablet or computer.

### It's Easy

1. Add your Regions credit card, debit card or Now Card — you only have to do this once.
2. Start shopping. When you're ready to pay, look for the Visa icon  at checkout and select the Regions card you'd like to use. You can skip guest checkout and bypass form fields.
3. Enter your user ID to complete your purchase. You won't need your password if you're shopping on a trusted device.

### It's Smart

No need to fill out credit card and shipping information every time you make a purchase. Just look for the Visa icon  at checkout to skip long forms and save time.

### It's Secure

No need to worry about identity theft or hacking. Your credit card information is stored behind multiple layers of security. Shop with confidence on any of your devices.

[Sign up today](#) to enjoy easy online checkout with fewer clicks.

(Source: <https://www.regions.com/digital-banking/transfer-money-and-pay/click-to-pay-with-visa>)





## Venture

# Earn 75,000 Bonus Miles

once you spend \$4,000 on purchases within the first 3 months from account opening

[Card Details](#)
[Security](#)
[FAQ](#)

(Source:

[https://applynow.capitalone.com/?productId=20309&external\\_id=WWW\\_XXXXX\\_XXX\\_SEM-Brand\\_MSN\\_ZZ\\_ZZ\\_T\\_Home\\_ZZ\\_5c41d4ea-bd50-4ced-a631-97fd8a8adeef\\_86361&msclkid=af4735f015e11dab0f00566108753338](https://applynow.capitalone.com/?productId=20309&external_id=WWW_XXXXX_XXX_SEM-Brand_MSN_ZZ_ZZ_T_Home_ZZ_5c41d4ea-bd50-4ced-a631-97fd8a8adeef_86361&msclkid=af4735f015e11dab0f00566108753338))

☰
CHASE CREDIT CARDS
Sign in

[Featured Cards](#)
[Card Finder](#)
[Card Categories](#)
[Card Brands](#)

# Rewards Credit Cards

Find the best rewards credit card for your lifestyle, whether you're looking to earn travel rewards or get cash back rewards while shopping. Compare our rewards cards' offers and bonuses to choose the right card for you.

Chase Freedom Unlimited<sup>®</sup> credit card

★★★★★  
(10,034 cardmember reviews)

## NEW CARDMEMBER OFFER

**\$200 bonus plus 5% grocery store offer - up to \$800 total cash back**

Earn a \$200 bonus after you spend \$500 on purchases in the first 3 months from account opening. Plus, earn 5% cash back on grocery store purchases (excluding Target<sup>3</sup> and Walmart<sup>3</sup>) on up to \$12,000 spent in the first year (that's \$600 cash back!).

## AT A GLANCE

**Earn cash back for every purchase.** Earn unlimited 1.5% cash back or more on all purchases, like 3% on dining and drugstores and 5% on travel purchased through Chase.

## APR

0% Intro APR for 15 months from account opening on purchases and balance transfers.<sup>1</sup> After the intro period, a variable APR of 18.74%-27.49%.<sup>1</sup> Balance transfer fee applies, see pricing and terms for more details.<sup>1</sup>

## ANNUAL FEE

\$0<sup>2</sup>










[Apply Now](#)
[Learn more >](#)

<sup>1</sup>[Pricing & Terms](#)  
<sup>2</sup>[Rewards Program Agreement \(PDF\)](#)


☐ Compare <sup>?</sup>

(Source: <https://creditcards.chase.com/rewards-credit-cards?CELL=6TKV>)












[Sign On](#)

[Featured](#)
[View All Cards](#)
[Balance Transfer](#)
[Cash Back](#)
[Rewards](#)
[Low Intro APR](#)
[Travel](#)
[Business](#)



**Costco Anywhere Visa® Card by Citi**  
Designed exclusively for Costco Members

**Earn 4% cash back on eligible gas and EV charging**  
For the first \$7,000 per year and then 1% thereafter.  
A Costco membership is required to apply.  
[Join Costco today.](#)

**Earn cash back on other purchases**  
3% cash back on restaurant and eligible travel purchases worldwide; 2% cash back on all other purchases from Costco and [Costco.com](#); 1% cash back on all other purchases.


**No Foreign Transaction Fees\***  
No matter where you're traveling, when you use your Costco Anywhere Visa® Card by Citi there are no foreign transaction fees on purchases.\*

[Apply Now](#)

[\\*Pricing & Information](#)

[See more details](#)

**Take your business to the next level**



**Costco Anywhere Visa® Business Card by Citi**  
Power your small business with the only business card for Costco Members

**Earn 4% cash back on eligible gas and EV charging**  
For the first \$7,000 per year and then 1% thereafter.  
A Costco membership is required to apply.  
[Join Costco today.](#)

**Earn cash back on other purchases**  
3% cash back on restaurant and eligible travel purchases worldwide; 2% cash back on all other purchases from Costco and [Costco.com](#); 1% cash back on all other purchases.

**No Foreign Transaction Fees\***  
No matter where you're traveling, when you use your Costco Anywhere Visa® Card by Citi there are no foreign transaction fees on purchases.\*

[Apply Now](#)

[\\*Pricing & Information](#)


[See more details](#)

(Source:

[https://citicards.citi.com/usc/Multi/Featured/default.htm?cmp=knc|acquire|2004|FCP|CARDS|U NK|MSN|BR&gclid=3d98efa69e8110b186bd8c37bc1d66e3&gclsrc=3p.ds&msclkid=3d98efa69 e8110b186bd8c37bc1d66e3&BT\\_TX=1&tab=all-cards](https://citicards.citi.com/usc/Multi/Featured/default.htm?cmp=knc|acquire|2004|FCP|CARDS|U NK|MSN|BR&gclid=3d98efa69e8110b186bd8c37bc1d66e3&gclsrc=3p.ds&msclkid=3d98efa69 e8110b186bd8c37bc1d66e3&BT_TX=1&tab=all-cards))

### 3 Core digital payment tokenization programs


There are three programs to choose from. Each program is described below and available on your dashboard after you create an account. You can apply to one or more based on your certification needs.



**Tokenization eCommerce and Card on File (card not present)**

Online payments continue to suffer worse authorization rates compared to in-store. By eliminating PAN storage and transfer, Visa Tokens help reduce data breach, mitigate fraud and create a trusted environment which can improve authorization rates for digital transactions.


[Apply Now](#)



**Click to Pay (Visa Secure Remote Commerce)**

Click to Pay was designed to deliver a fast, easy, and secure digital guest checkout experience by eliminating passwords and tedious form fill. By making the payment experience more streamlined and consistent across digital channels, we look to reduce cart abandonment and drive higher conversion.

[Apply Now](#)



**Tokenization - TSP (card present)**

Whether it's a mobile phone or other payment-enabled devices, Visa's Tokens enable payments to be made with the wave of a hand. We're partnering with mobile wallets, device manufacturers, and platform providers to create a convenient, secure, and touch-free way to pay at point-of-sale.

[Apply Now](#)

(Source: <https://partner.visa.com/site/programs/visa-ready/digital-payments.html>)

## All you need to know about Tokenization

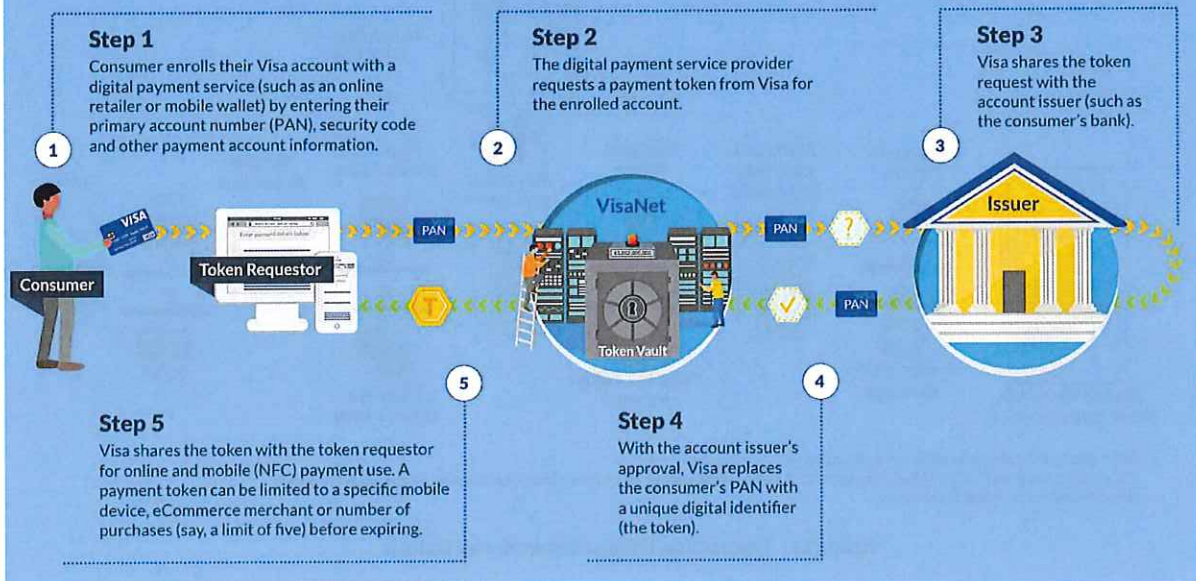
Visa Token Service, a new security technology from Visa, replaces sensitive account information, such as the 16-digit account number, with a unique digital identifier called a *token*. The token allows payments to be processed without exposing actual account details that could potentially be compromised.



(Source: <https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf>)

## How Visa Token Service Works

The Visa Token Service enables digital payment service providers and financial institutions to offer their customers a safe way to shop online and with mobile devices. Here's how a token is initiated.

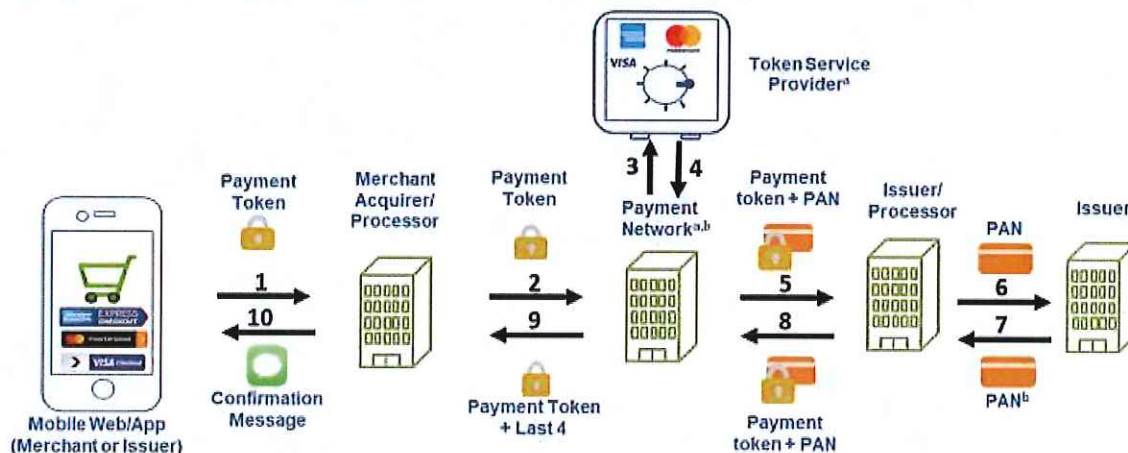


(Source: <https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf>)



### 5.3 Transaction Processing (Network Pay Button)

Figure 11 illustrates the processing for tokenized transactions using a mobile phone with a network pay button. Note that not all transactions with pay buttons will be tokenized.



<sup>a</sup> See Section 7 for information on debit routing.

<sup>b</sup> "Payment Network" is the token requester and refers to the network of the primary card brand of the card for which detokenization is being requested.

**Figure 11. Transaction Using a Network Pay Button**

During the transaction process, the following steps occur:

1. The cardholder uses a mobile app or web browser interface at checkout and selects to pay using a cloud-based wallet. The cardholder is redirected to the cloud wallet server for authentication. The cardholder verifies the amount and selects the token for payment. The cardholder is redirected to the mobile application or web with a payment transaction identifier.<sup>7</sup> The payment transaction identifier is passed to merchant's back office to complete the payment

<sup>7</sup> The payment transaction identifier is a unique number identifying a transaction the customer has accepted on the cloud wallet server. It does not include a token or cryptogram data.

process. The merchant's back office uses the payment transaction identifier to obtain a token and cryptogram from the cloud wallet server. The merchant's back office sends the token and cryptogram to the merchant acquirer/processor.

2. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that this transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to a clear PAN.
4. The TSP verifies the cryptogram and returns the clear PAN to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor sends the transaction response to the mobile application. The merchant's back office confirms payment status to the cloud wallet server.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

59. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, an account holder of Defendant (or an account holder of a bank using Visa tokenization services) requests Defendant to provision a specific debit and/or credit card for use with Visa tokenization services. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder using his or her Visa tokenization information. In initiating the request, the account holder's smartphone, mobile app, or web browser receives certain transaction specific information from the merchant, which is incorporated into a cryptogram generated by a server

that is transmitted to the merchant, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted to the merchant. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

60. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by a cardholder of a debit and/or credit card of Defendant (or a bank using Visa tokenization services) for provisioning a specific debit and/or credit card of Defendant (or a bank using Visa tokenization services) for use of Visa tokenization services. The messaging gateway is also programmed to receive requests initiated by a cardholder customer of Defendant (or a bank using Visa tokenization services) for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder. This messaging gateway is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

61. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the messaging



gateway and in secure communication therewith is an authorization server that processes the received request to identify the token value sent for the account selected to be charged that was passed to the merchant. From the token value, the server can look up the debit and/or credit card account number. The authorization server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to provide the authentication services.

62. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive within the payment authorization request transaction specific information that was input into the request by the merchant. The interface is either hosted directly by Defendants or through an agent with whom Defendants have contracted to provide the authentication services.

63. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

64. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

65. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

66. Defendants thus infringe one or more of the claims of the 079 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 079 Patent. Thus, Defendants' use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 079 Patent.

67. Defendants have directly infringed and continue to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(a), by making, using, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

68. Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by others and Defendants will continue to do so unless enjoined by this Court. Defendants' deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses,

distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Defendants knew and/or were willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

69. Defendants continue to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continue to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

70. Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 079 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.



71. Defendants have committed these acts of infringement without license or authorization.

72. By engaging in the conduct described herein, Defendants have caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Defendants are thus liable to Textile for infringement of the 079 Patent, pursuant to 35 U.S.C. § 271.

73. As a direct and proximate result of Defendants' infringement of the 079 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Defendants' past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

74. In addition, the infringing acts and practices of Defendants have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Textile is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Defendants are finally and permanently enjoined from further infringement.

75. Regions has had actual knowledge of the 079 Patent at least as of October 18, 2013, when Textile sent a letter to Grayson Hall, Jr., then Chief Executive Officer of Regions Bank, that described certain implementations of the patented technology and specifically identified the 079 Patent.

76. Regions has had actual knowledge of the 079 Patent at least as of November 10, 2014, when Textile sent a letter to Grayson Hall, Jr., then Chief Executive Officer of Regions

Bank, that described certain implementations of the patented technology and specifically identified the 079 Patent.

77. Capital One has had actual knowledge of the 079 Patent at least as of October 18, 2013, when Textile sent a letter to Richard D. Fairbank, then CEO of Capital One, that described certain implementations of the patented technology and specifically identified the 079 Patent.

78. Capital One has had actual knowledge of the 079 Patent at least as of November 10, 2014, when Textile sent a letter to Richard D. Fairbank, then CEO of Capital One, that described certain implementations of the patented technology and specifically identified the 079 Patent.

79. Chase has had actual knowledge of the 079 Patent at least as of November 28, 2014, when Textile sent a letter to James Dimon, then CEO of Chase Bank, that described certain implementations of the patented technology and specifically identified the 079 Patent.

80. Citibank has had actual knowledge of the 079 Patent at least as of November 28, 2014, when Textile sent letters to Michael Corbat, then CEO of Citigroup, Jud Linville, then CEO as to Citi Cards at Citigroup, Barbara Desoer, then CEO of Citibank, N.A., and William J. Mills, then CEO as to North America at Citigroup, that described certain implementations of the patented technology and specifically identified the 079 Patent.

81. Visa has had actual knowledge of the 079 Patent at least as of July 10, 2014, when Textile sent letters to John M. Partridge, then President of Visa U.S.A. Inc., and Joseph W. Saunders, then Chairman and CEO of Visa U.S.A. Inc., that described certain implementations of the patented technology and specifically identified the 079 Patent.

82. Visa has had actual knowledge of the 079 Patent at least as of August 29, 2014, when Textile sent letters to Charles W. Scharf, then CEO of Visa Inc., Elizabeth Buse, then

Global Executive, Solutions at Visa Inc., Antonio Lucio, then Chief Brand Officer of Visa Inc., Jim McCarthy, then Global Head / SVP of Innovation & Strategic Partnerships of Visa Inc., Ryan McInerney, then President of Visa Inc., Byron H. Pollitt, then CFO of Visa Inc., Ellen Richey, then Chief Enterprise Risk Officer of Visa Inc., and Rajat Taneja, then Executive Vice President, Technology, at Visa Inc., that described certain implementations of the patented technology and specifically identified the 079 Patent.

83. Visa has had actual knowledge of the 079 Patent at least as of November 10, 2014, when Textile sent letters to Charles W. Scharf, then CEO of Visa Inc., Elizabeth Buse, then Global Executive, Solutions at Visa Inc., Antonio Lucio, then Chief Brand Officer of Visa Inc., Jim McCarthy, then Global Head / SVP of Innovation & Strategic Partnerships of Visa Inc., Ryan McInerney, then President of Visa Inc., Byron H. Pollitt, then CFO of Visa Inc., Ellen Richey, then Chief Enterprise Risk Officer of Visa Inc., and Rajat Taneja, then Executive Vice President, Technology, at Visa Inc., that described certain implementations of the patented technology and specifically identified the 079 Patent.

84. Visa has had actual knowledge of the 079 Patent at least as of April 14, 2015, when Textile sent letters to Charles W. Scharf, then CEO of Visa Inc., Elizabeth Buse, then Global Executive, Solutions at Visa Inc., Antonio Lucio, then Chief Brand Officer of Visa Inc., Jim McCarthy, then Global Head / SVP of Innovation & Strategic Partnerships of Visa Inc., Ryan McInerney, then President of Visa Inc., Byron H. Pollitt, then CFO of Visa Inc., Ellen Richey, then Chief Enterprise Risk Officer of Visa Inc., and Rajat Taneja, then Executive Vice President, Technology, at Visa Inc., that described certain implementations of the patented technology and specifically identified the 079 Patent.



85. Defendants have had actual knowledge of the 079 Patent at least as of the date when they were notified of the filing of this action. By the time of trial, Defendants will have known and intended (since receiving such notice) that their continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 079 Patent.

86. Defendants have also indirectly and willfully infringed, and continue to indirectly and willfully infringe, the 079 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

87. Textile has been damaged as a result of the infringing conduct by Defendants alleged above. Thus, Defendants are liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

88. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 079 Patent.

## **COUNT II**

### **INFRINGEMENT OF U.S. PATENT NO. 8,533,802**

89. On September 10, 2013, United States Patent No. 8,533,802 (“the 802 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

90. Textile is the owner of the 802 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 802 Patent against infringers, and to collect damages for all relevant times.

91. Regions, Capital One, Chase, and Citibank offer Visa-branded debit and/or credit cards, such as the Regions Visa Debit Card, various Regions Visa Credit Cards, the Capital One

Venture X Visa Credit Card, the Capital One Venture Visa Credit Card, the Capital One Journey Visa Credit Card, the Chase Freedom Unlimited Visa Credit Card, the Chase Sapphire Preferred Visa Credit Card, the Chase Sapphire Reserve Visa Credit Card, the Citibank Costco Anywhere Visa Credit Card, and the Citibank Costco Anywhere Visa Business Credit Card, that are used with Regions, Capital One, Chase, and/or Citibank authentication systems that authenticate the identity of a Regions, Capital One, Chase, or Citibank card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). Visa provides tokenization and processing services to banks for the purposes of using the Accused Instrumentality card authentication system. The Accused Instrumentality card authentication systems that are used, made, and sold by Regions, Capital One, Chase, Citibank, and Visa are implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones or computers and use those tokens, which are generated and communicated by the system, and wherein each account held by the user has its own token.


## Click to Pay with Visa

*Transfer Money and Pay*




Click to Pay with Visa<sup>1</sup> is the easy, smart and secure way to shop online with your smartphone, tablet or computer.

### It's Easy

1. Add your Regions credit card, debit card or Now Card — you only have to do this once.
2. Start shopping. When you're ready to pay, look for the Visa icon  at checkout and select the Regions card you'd like to use. You can skip guest checkout and bypass form fields.
3. Enter your user ID to complete your purchase. You won't need your password if you're shopping on a trusted device.

### It's Smart

No need to fill out credit card and shipping information every time you make a purchase. Just look for the Visa icon  at checkout to skip long forms and save time.

### It's Secure

No need to worry about identity theft or hacking. Your credit card information is stored behind multiple layers of security. Shop with confidence on any of your devices.

[Sign up today](#) to enjoy easy online checkout with fewer clicks.

(Source: <https://www.regions.com/digital-banking/transfer-money-and-pay/click-to-pay-with-visa>)





## Venture Earn 75,000 Bonus Miles

once you spend \$4,000 on purchases within the first 3 months from account opening

Card Details

Security

FAQ

(Source:

[https://applynow.capitalone.com/?productId=20309&external\\_id=WWW\\_XXXXX\\_XXX\\_SEM-Brand\\_MSN\\_ZZ\\_ZZ\\_T\\_Home\\_ZZ\\_5c41d4ea-bd50-4ced-a631-97fd8a8adeef\\_86361&mssclkid=af4735f015e11dab0f00566108753338](https://applynow.capitalone.com/?productId=20309&external_id=WWW_XXXXX_XXX_SEM-Brand_MSN_ZZ_ZZ_T_Home_ZZ_5c41d4ea-bd50-4ced-a631-97fd8a8adeef_86361&mssclkid=af4735f015e11dab0f00566108753338))

**CHASE CREDIT CARDS** Sign in

Featured Cards | Card Finder | Card Categories | Card Brands

## Rewards Credit Cards

Find the best rewards credit card for your lifestyle, whether you're looking to earn travel rewards or get cash back rewards while shopping. Compare our rewards cards' offers and bonuses to choose the right card for you.

### Chase Freedom Unlimited<sup>®</sup> credit card



★★★★★  
(10,034 cardmember reviews)

#### NEW CARDMEMBER OFFER

#### \$200 bonus plus 5% grocery store offer - up to \$800 total cash back

Earn a \$200 bonus after you spend \$500 on purchases in the first 3 months from account opening. Plus, earn 5% cash back on grocery store purchases (excluding Target<sup>1</sup> and Walmart<sup>2</sup>) on up to \$12,000 spent in the first year (that's \$600 cash back!).

#### AT A GLANCE

Earn cash back for every purchase. Earn unlimited 1.5% cash back or more on all purchases, like 3% on dining and drugstores and 5% on travel purchased through Chase.

#### APR

0% Intro APR for 15 months from account opening on purchases and balance transfers.<sup>‡</sup> After the intro period, a variable APR of 18.74%-27.49%.<sup>‡</sup> Balance transfer fee applies, see pricing and terms for more details.<sup>‡</sup>

#### ANNUAL FEE

\$0<sup>‡</sup>










[Apply Now](#)

[Learn more >](#)


[Pricing & Terms](#)  
[Rewards Program Agreement \(PDF\)](#)

☐ [Compare](#)

(Source: <https://creditcards.chase.com/rewards-credit-cards?CELL=6TKV>)










[Sign On](#)

Featured View All Cards Balance Transfer Cash Back Rewards Low Intro APR Travel Business



**Costco Anywhere Visa® Card by Citi**  
Designed exclusively for Costco Members

**Earn 4% cash back on eligible gas and EV charging**  
For the first \$7,000 per year and then 1% thereafter.  
A Costco membership is required to apply.  
[Join Costco today.](#)

**Earn cash back on other purchases**  
3% cash back on restaurant and eligible travel purchases worldwide, 2% cash back on all other purchases from Costco and [Costco.com](#), 1% cash back on all other purchases.


**No Foreign Transaction Fees\***  
No matter where you're traveling, when you use your Costco Anywhere Visa® Card by Citi there are no foreign transaction fees on purchases.\*

[Apply Now](#)

[\\*Pricing & Information](#)

[See more details](#)

Take your business to the next level



**Costco Anywhere Visa® Business Card by Citi**  
Power your small business with the only business card for Costco Members

**Earn 4% cash back on eligible gas and EV charging**  
For the first \$7,000 per year and then 1% thereafter.  
A Costco membership is required to apply.  
[Join Costco today.](#)

**Earn cash back on other purchases**  
3% cash back on restaurant and eligible travel purchases worldwide, 2% cash back on all other purchases from Costco and [Costco.com](#), 1% cash back on all other purchases.

**No Foreign Transaction Fees\***  
No matter where you're traveling, when you use your Costco Anywhere Visa® Card by Citi there are no foreign transaction fees on purchases.\*

[Apply Now](#)

[\\*Pricing & Information](#)


[See more details](#)

(Source:

[https://citicards.citi.com/usc/Multi/Featured/default.htm?cmp=knc|acquire|2004|FCP|CARDS|U NK|MSN|BR&gclid=3d98efa69e8110b186bd8c37bc1d66e3&gclsrc=3p.ds&msclkid=3d98efa69 e8110b186bd8c37bc1d66e3&BT\\_TX=1&tab=all-cards](https://citicards.citi.com/usc/Multi/Featured/default.htm?cmp=knc|acquire|2004|FCP|CARDS|U NK|MSN|BR&gclid=3d98efa69e8110b186bd8c37bc1d66e3&gclsrc=3p.ds&msclkid=3d98efa69 e8110b186bd8c37bc1d66e3&BT_TX=1&tab=all-cards))

### 3 Core digital payment tokenization programs


There are three programs to choose from. Each program is described below and available on your dashboard after you create an account. You can apply to one or more based on your certification needs.



**Tokenization eCommerce and Card on File (card not present)**

Online payments continue to suffer worse authorization rates compared to in-store. By eliminating PAN storage and transfer, Visa Tokens help reduce data breach, mitigate fraud and create a trusted environment which can improve authorization rates for digital transactions.


[Apply Now](#)



**Click to Pay (Visa Secure Remote Commerce)**

Click to Pay was designed to deliver a fast, easy, and secure digital guest checkout experience by eliminating passwords and tedious form fill. By making the payment experience more streamlined and consistent across digital channels, we look to reduce cart abandonment and drive higher conversion.

[Apply Now](#)



**Tokenization - TSP (card present)**

Whether it's a mobile phone or other payment-enabled devices, Visa's Tokens enable payments to be made with the wave of a hand. We're partnering with mobile wallets, device manufacturers, and platform providers to create a convenient, secure, and touch-free way to pay at point-of-sale.

[Apply Now](#)

(Source: <https://partner.visa.com/site/programs/visa-ready/digital-payments.html>)

## All you need to know about Tokenization

Visa Token Service, a new security technology from Visa, replaces sensitive account information, such as the 16-digit account number, with a unique digital identifier called a *token*. The token allows payments to be processed without exposing actual account details that could potentially be compromised.

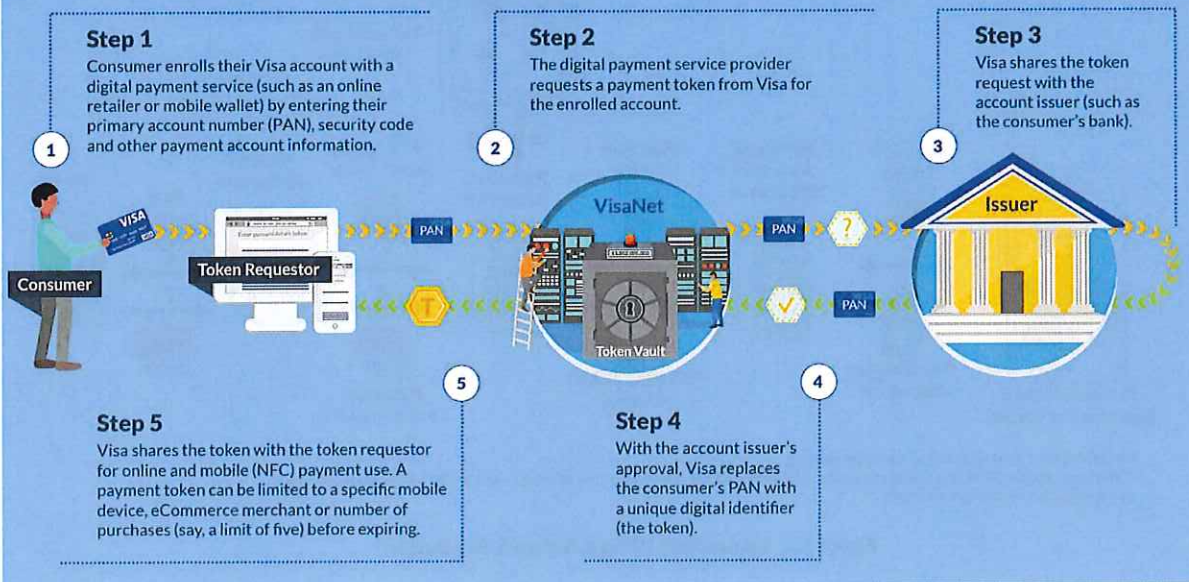


(Source: <https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf>)



## How Visa Token Service Works

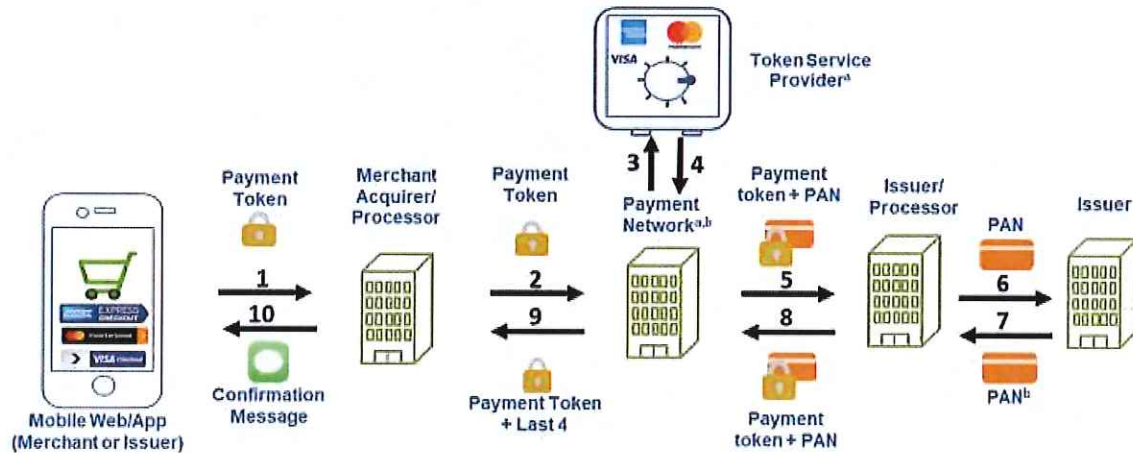
The Visa Token Service enables digital payment service providers and financial institutions to offer their customers a safe way to shop online and with mobile devices. Here's how a token is initiated.



(Source: <https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf>)

### 5.3 Transaction Processing (Network Pay Button)

Figure 11 illustrates the processing for tokenized transactions using a mobile phone with a network pay button. Note that not all transactions with pay buttons will be tokenized.



<sup>a</sup> See Section 7 for information on debit routing.

<sup>b</sup> "Payment Network" is the token requester and refers to the network of the primary card brand of the card for which detokenization is being requested.

**Figure 11. Transaction Using a Network Pay Button**

During the transaction process, the following steps occur:

1. The cardholder uses a mobile app or web browser interface at checkout and selects to pay using a cloud-based wallet. The cardholder is redirected to the cloud wallet server for authentication. The cardholder verifies the amount and selects the token for payment. The cardholder is redirected to the mobile application or web with a payment transaction identifier.<sup>7</sup> The payment transaction identifier is passed to merchant's back office to complete the payment

<sup>7</sup> The payment transaction identifier is a unique number identifying a transaction the customer has accepted on the cloud wallet server. It does not include a token or cryptogram data.

process. The merchant's back office uses the payment transaction identifier to obtain a token and cryptogram from the cloud wallet server. The merchant's back office sends the token and cryptogram to the merchant acquirer/processor.

2. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant),
3. The payment network determines that this transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to a clear PAN.
4. The TSP verifies the cryptogram and returns the clear PAN to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor sends the transaction response to the mobile application. The merchant's back office confirms payment status to the cloud wallet server.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

92. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, an account holder of Defendant (or an account holder of a bank using Visa tokenization services) requests Defendant to provision a specific debit and/or credit card for use with Visa tokenization services. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder using his or her Visa tokenization information. In initiating the request, the account holder's smartphone, mobile app, or web browser receives certain transaction specific information from the merchant, which is incorporated into a cryptogram generated by a server



that is transmitted to the merchant, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted to the merchant. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

93. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by a cardholder of a debit and/or credit card of Defendant (or a bank using Visa tokenization services) for provisioning a specific debit and/or credit card of Defendant (or a bank using Visa tokenization services) for use of Visa tokenization services. This messaging gateway is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

94. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate a key string adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the messaging gateway and in secure communication therewith is an authorization server that generates a token corresponding to the debit and/or credit card account number. The authorization server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to provide the authentication services.

95. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive transaction specific information that was input into the request by the merchant, *e.g.*, the merchant ID, invoice number, invoice amount, and date/timestamp. The interface is either hosted directly by Defendants or through an agent with whom Defendants have contracted to provide the authentication services.

96. The Accused Instrumentality includes a first set of instructions further operable to communicate the key string to the authorized user that the requester purports to be. For example, the messaging gateway sends the generated token to the authorized user's smartphone, mobile app, or web browser for use in merchant transactions.

97. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

98. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

99. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

100. Defendants thus infringe one or more claims of the 802 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 802 Patent. Thus, Defendants' use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 802 Patents.

101. Defendants have directly infringed and continue to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

102. Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and Defendants will continue to do so unless enjoined by this Court. Defendants' deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing



the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Defendants knew and/or were willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

103. Defendants continue to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continue to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

104. Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 802 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

105. Defendants have committed these acts of infringement without license or authorization.

106. By engaging in the conduct described herein, Defendants have caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Defendants are thus liable to Textile for infringement of the 802 Patent, pursuant to 35 U.S.C. § 271.

107. As a direct and proximate result of Defendants' infringement of the 802 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Defendants' past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

108. In addition, the infringing acts and practices of Defendants have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Textile is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Defendants are finally and permanently enjoined from further infringement.

109. Regions has had actual knowledge of the 802 Patent at least as of October 18, 2013, when Textile sent a letter to Grayson Hall, Jr., then Chief Executive Officer of Regions Bank, that described certain implementations of the patented technology and specifically identified the 802 Patent.

110. Regions has had actual knowledge of the 802 Patent at least as of November 10, 2014, when Textile sent a letter to Grayson Hall, Jr., then Chief Executive Officer of Regions

Bank, that described certain implementations of the patented technology and specifically identified the 802 Patent.

111. Capital One has had actual knowledge of the 802 Patent at least as of October 18, 2013, when Textile sent a letter to Richard D. Fairbank, then CEO of Capital One, that described certain implementations of the patented technology and specifically identified the 802 Patent.

112. Capital One has had actual knowledge of the 802 Patent at least as of November 10, 2014, when Textile sent a letter to Richard D. Fairbank, then CEO of Capital One, that described certain implementations of the patented technology and specifically identified the 802 Patent.

113. Chase has had actual knowledge of the 802 Patent at least as of November 28, 2014, when Textile sent a letter to James Dimon, then CEO of Chase Bank, that described certain implementations of the patented technology and specifically identified the 802 Patent.

114. Citibank has had actual knowledge of the 802 Patent at least as of November 28, 2014, when Textile sent letters to Michael Corbat, then CEO of Citigroup, Jud Linville, then CEO as to Citi Cards at Citigroup, Barbara Desoer, then CEO of Citibank, N.A., and William J. Mills, then CEO as to North America at Citigroup, that described certain implementations of the patented technology and specifically identified the 802 Patent.

115. Visa has had actual knowledge of the 802 Patent at least as of July 10, 2014, when Textile sent letters to John M. Partridge, then President of Visa U.S.A. Inc., and Joseph W. Saunders, then Chairman and CEO of Visa U.S.A. Inc., that described certain implementations of the patented technology and specifically identified the 802 Patent.

116. Visa has had actual knowledge of the 802 Patent at least as of August 29, 2014, when Textile sent letters to Charles W. Scharf, then CEO of Visa Inc., Elizabeth Buse, then



Global Executive, Solutions at Visa Inc., Antonio Lucio, then Chief Brand Officer of Visa Inc., Jim McCarthy, then Global Head / SVP of Innovation & Strategic Partnerships of Visa Inc., Ryan McInerney, then President of Visa Inc., Byron H. Pollitt, then CFO of Visa Inc., Ellen Richey, then Chief Enterprise Risk Officer of Visa Inc., and Rajat Taneja, then Executive Vice President, Technology, at Visa Inc., that described certain implementations of the patented technology and specifically identified the 802 Patent.

117. Visa has had actual knowledge of the 802 Patent at least as of November 10, 2014, when Textile sent letters to Charles W. Scharf, then CEO of Visa Inc., Elizabeth Buse, then Global Executive, Solutions at Visa Inc., Antonio Lucio, then Chief Brand Officer of Visa Inc., Jim McCarthy, then Global Head / SVP of Innovation & Strategic Partnerships of Visa Inc., Ryan McInerney, then President of Visa Inc., Byron H. Pollitt, then CFO of Visa Inc., Ellen Richey, then Chief Enterprise Risk Officer of Visa Inc., and Rajat Taneja, then Executive Vice President, Technology, at Visa Inc., that described certain implementations of the patented technology and specifically identified the 802 Patent.

118. Visa has had actual knowledge of the 802 Patent at least as of April 14, 2015, when Textile sent letters to Charles W. Scharf, then CEO of Visa Inc., Elizabeth Buse, then Global Executive, Solutions at Visa Inc., Antonio Lucio, then Chief Brand Officer of Visa Inc., Jim McCarthy, then Global Head / SVP of Innovation & Strategic Partnerships of Visa Inc., Ryan McInerney, then President of Visa Inc., Byron H. Pollitt, then CFO of Visa Inc., Ellen Richey, then Chief Enterprise Risk Officer of Visa Inc., and Rajat Taneja, then Executive Vice President, Technology, at Visa Inc., that described certain implementations of the patented technology and specifically identified the 802 Patent.

119. Defendants have had actual knowledge of the 802 Patent at least as of the date when they were notified of the filing of this action. By the time of trial, Defendants will have known and intended (since receiving such notice) that their continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 802 Patent.

120. Defendants have also indirectly and willfully infringed, and continue to indirectly and willfully infringe, the 802 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

121. Textile has been damaged as a result of the infringing conduct by Defendants alleged above. Thus, Defendants are liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

122. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 802 Patent.

### **COUNT III**

#### **INFRINGEMENT OF U.S. PATENT NO. 10,148,659**

123. On December 4, 2018, United States Patent No. 10,148,659 (“the 659 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

124. Textile is the owner of the 659 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 659 Patent against infringers, and to collect damages for all relevant times.

125. Regions, Capital One, Chase, and Citibank offer Visa-branded debit and/or credit cards, such as the Regions Visa Debit Card, various Regions Visa Credit Cards, the Capital One

Venture X Visa Credit Card, the Capital One Venture Visa Credit Card, the Capital One Journey Visa Credit Card, the Chase Freedom Unlimited Visa Credit Card, the Chase Sapphire Preferred Visa Credit Card, the Chase Sapphire Reserve Visa Credit Card, the Citibank Costco Anywhere Visa Credit Card, and the Citibank Costco Anywhere Visa Business Credit Card, that are used with Regions, Capital One, Chase, and/or Citibank computer-implemented systems for a credit or debit and/or credit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit and/or credit card account number to the merchant (the “Accused Instrumentality”). Visa provides tokenization services to banks for the purposes of using the Accused Instrumentality transaction-specific access authorization system. The Accused Instrumentality transaction-specific access authorization systems that are used, made, and sold by Regions, Capital One, Chase, Citibank, and Visa are implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones or computers and use those tokens, which are generated and communicated by the system, and wherein each account held by the user has its own token.




## Click to Pay with Visa

*Transfer Money and Pay*




Click to Pay with Visa<sup>1</sup> is the easy, smart and secure way to shop online with your smartphone, tablet or computer.

### It's Easy

1. Add your Regions credit card, debit card or Now Card — you only have to do this once.
2. Start shopping. When you're ready to pay, look for the Visa icon  at checkout and select the Regions card you'd like to use. You can skip guest checkout and bypass form fields.
3. Enter your user ID to complete your purchase. You won't need your password if you're shopping on a trusted device.

### It's Smart

No need to fill out credit card and shipping information every time you make a purchase. Just look for the Visa icon  at checkout to skip long forms and save time.

### It's Secure

No need to worry about identity theft or hacking. Your credit card information is stored behind multiple layers of security. Shop with confidence on any of your devices.

[Sign up today](#) to enjoy easy online checkout with fewer clicks.

(Source: <https://www.regions.com/digital-banking/transfer-money-and-pay/click-to-pay-with-visa>)



## Venture Earn 75,000 Bonus Miles

once you spend \$4,000 on purchases within the first 3 months from account opening

[Card Details](#) [Security](#) [FAQ](#)

(Source:

[https://applynow.capitalone.com/?productId=20309&external\\_id=WWW\\_XXXXX\\_XXX\\_SEM-Brand\\_MSN\\_ZZ\\_ZZ\\_T\\_Home\\_ZZ\\_5c41d4ea-bd50-4ced-a631-97fd8a8adeef\\_86361&msclkid=af4735f015e11dab0f00566108753338](https://applynow.capitalone.com/?productId=20309&external_id=WWW_XXXXX_XXX_SEM-Brand_MSN_ZZ_ZZ_T_Home_ZZ_5c41d4ea-bd50-4ced-a631-97fd8a8adeef_86361&msclkid=af4735f015e11dab0f00566108753338))

**CHASE CREDIT CARDS** [Sign in](#)

[Featured Cards](#) | [Card Finder](#) | [Card Categories](#) | [Card Brands](#)

## Rewards Credit Cards

Find the best rewards credit card for your lifestyle, whether you're looking to earn travel rewards or get cash back rewards while shopping. Compare our rewards cards' offers and bonuses to choose the right card for you.

### Chase Freedom Unlimited<sup>®</sup> credit card



★★★★★  
(10,034 cardmember reviews)

#### NEW CARDMEMBER OFFER

#### \$200 bonus plus 5% grocery store offer - up to \$800 total cash back

Earn a \$200 bonus after you spend \$500 on purchases in the first 3 months from account opening. Plus, earn 5% cash back on grocery store purchases (excluding Target<sup>®</sup> and Walmart<sup>®</sup>) on up to \$12,000 spent in the first year (that's \$600 cash back!).

#### AT A GLANCE

Earn cash back for every purchase. Earn unlimited 1.5% cash back or more on all purchases, like 3% on dining and drugstores and 5% on travel purchased through Chase.

#### APR

0% Intro APR for 15 months from account opening on purchases and balance transfers.<sup>‡</sup> After the Intro period, a variable APR of 18.74%-27.49%.<sup>‡</sup> Balance transfer fee applies, see pricing and terms for more details.<sup>‡</sup>

#### ANNUAL FEE

\$0<sup>‡</sup>










[Apply Now](#)

[Learn more >](#)


[Pricing & Terms](#)  
[Rewards Program Agreement \(PDF\)](#)

☐ [Compare](#) [?](#)

(Source: <https://creditcards.chase.com/rewards-credit-cards?CELL=6TKV>)










[Sign On](#)

Featured View All Cards Balance Transfer Cash Back Rewards Low Intro APR Travel Business



**Costco Anywhere Visa® Card by Citi**  
Designed exclusively for Costco Members

**Earn 4% cash back on eligible gas and EV charging**  
For the first \$7,000 per year and then 1% thereafter.  
A Costco membership is required to apply.  
[Join Costco today.](#)

**Earn cash back on other purchases**  
3% cash back on restaurant and eligible travel purchases worldwide. 2% cash back on all other purchases from Costco and [Costco.com](#). 1% cash back on all other purchases.


**No Foreign Transaction Fees\***  
No matter where you're traveling, when you use your Costco Anywhere Visa® Card by Citi there are no foreign transaction fees on purchases.\*

[Apply Now](#)

[\\*Pricing & Information](#)

[See more details](#)

**Take your business to the next level**



**Costco Anywhere Visa® Business Card by Citi**  
Power your small business with the only business card for Costco Members

**Earn 4% cash back on eligible gas and EV charging**  
For the first \$7,000 per year and then 1% thereafter.  
A Costco membership is required to apply.  
[Join Costco today.](#)

**Earn cash back on other purchases**  
3% cash back on restaurant and eligible travel purchases worldwide. 2% cash back on all other purchases from Costco and [Costco.com](#). 1% cash back on all other purchases.

**No Foreign Transaction Fees\***  
No matter where you're traveling, when you use your Costco Anywhere Visa® Card by Citi there are no foreign transaction fees on purchases.\*

[Apply Now](#)

[\\*Pricing & Information](#)

[See more details](#)


(Source:

[https://citicards.citi.com/usc/Multi/Featured/default.htm?cmp=knc|acquire|2004|FCP|CARDS|U NK|MSN|BR&gclid=3d98efa69e8110b186bd8c37bc1d66e3&gclsrc=3p.ds&msclkid=3d98efa69 e8110b186bd8c37bc1d66e3&BT\\_TX=1&tab=all-cards](https://citicards.citi.com/usc/Multi/Featured/default.htm?cmp=knc|acquire|2004|FCP|CARDS|U NK|MSN|BR&gclid=3d98efa69e8110b186bd8c37bc1d66e3&gclsrc=3p.ds&msclkid=3d98efa69 e8110b186bd8c37bc1d66e3&BT_TX=1&tab=all-cards))



### 3 Core digital payment tokenization programs


There are three programs to choose from. Each program is described below and available on your dashboard after you create an account. You can apply to one or more based on your certification needs.



**Tokenization eCommerce and Card on File (card not present)**

Online payments continue to suffer worse authorization rates compared to in-store. By eliminating PAN storage and transfer, Visa Tokens help reduce data breach, mitigate fraud and create a trusted environment which can improve authorization rates for digital transactions.


[Apply Now](#)



**Click to Pay (Visa Secure Remote Commerce)**

Click to Pay was designed to deliver a fast, easy, and secure digital guest checkout experience by eliminating passwords and tedious form fill. By making the payment experience more streamlined and consistent across digital channels, we look to reduce cart abandonment and drive higher conversion.

[Apply Now](#)



**Tokenization - TSP (card present)**

Whether it's a mobile phone or other payment-enabled devices, Visa's Tokens enable payments to be made with the wave of a hand. We're partnering with mobile wallets, device manufacturers, and platform providers to create a convenient, secure, and touch-free way to pay at point-of-sale.

[Apply Now](#)

(Source: <https://partner.visa.com/site/programs/visa-ready/digital-payments.html>)

## All you need to know about Tokenization

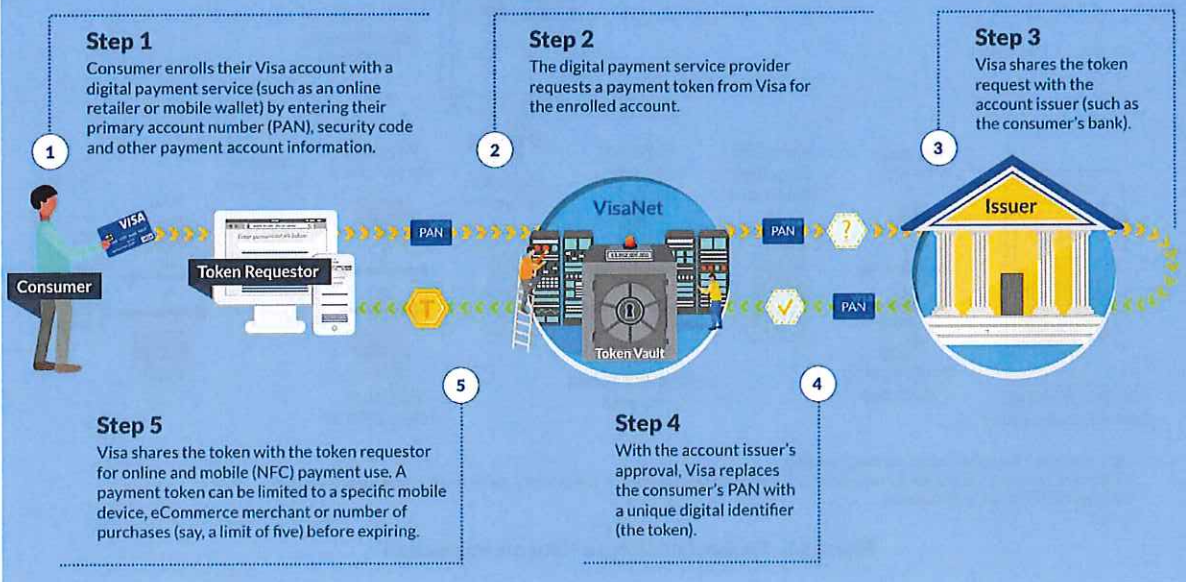
Visa Token Service, a new security technology from Visa, replaces sensitive account information, such as the 16-digit account number, with a unique digital identifier called a *token*. The token allows payments to be processed without exposing actual account details that could potentially be compromised.



(Source: <https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf>)

## How Visa Token Service Works

The Visa Token Service enables digital payment service providers and financial institutions to offer their customers a safe way to shop online and with mobile devices. Here's how a token is initiated.



(Source: <https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf>)

### 5.3 Transaction Processing (Network Pay Button)

Figure 11 illustrates the processing for tokenized transactions using a mobile phone with a network pay button. Note that not all transactions with pay buttons will be tokenized.

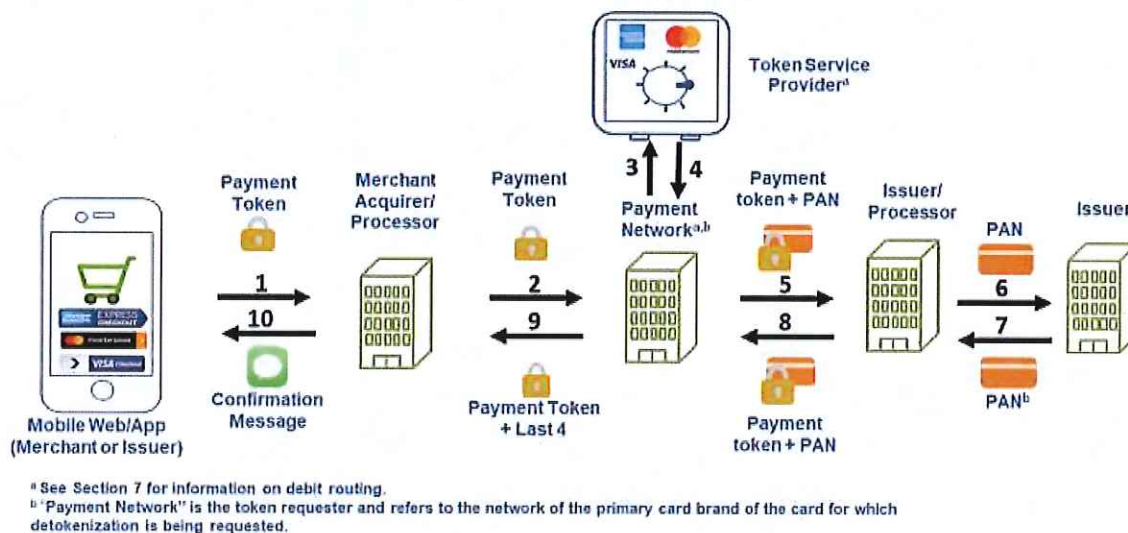


Figure 11. Transaction Using a Network Pay Button

During the transaction process, the following steps occur:

1. The cardholder uses a mobile app or web browser interface at checkout and selects to pay using a cloud-based wallet. The cardholder is redirected to the cloud wallet server for authentication. The cardholder verifies the amount and selects the token for payment. The cardholder is redirected to the mobile application or web with a payment transaction identifier.<sup>7</sup> The payment transaction identifier is passed to merchant's back office to complete the payment

<sup>7</sup> The payment transaction identifier is a unique number identifying a transaction the customer has accepted on the cloud wallet server. It does not include a token or cryptogram data.



process. The merchant's back office uses the payment transaction identifier to obtain a token and cryptogram from the cloud wallet server. The merchant's back office sends the token and cryptogram to the merchant acquirer/processor.

2. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that this transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to a clear PAN.
4. The TSP verifies the cryptogram and returns the clear PAN to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor sends the transaction response to the mobile application. The merchant's back office confirms payment status to the cloud wallet server.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

126. The Accused Instrumentality includes a computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant. For example, an account holder of Defendant (or an account holder of a bank using Visa tokenization services) requests Defendant to provision a specific debit and/or credit card for use with Visa tokenization services. The account holder can then request for payment to be made by Defendant (or a bank using Visa tokenization services) to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder using his or her Visa tokenization information. In

initiating the request, the account holder's smartphone, mobile app, or web browser receives certain transaction specific information from the merchant, which is incorporated into a cryptogram generated by a server that is transmitted to the merchant, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted to the merchant. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

127. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with an account holder's mobile device, a merchant's payment application, server, and/or other software or hardware, or both. The interface is also programmed to receive requests initiated by a cardholder customer of Defendant (or a bank using Visa tokenization services) for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder. This interface is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

128. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier

and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card and the debit and/or credit card account number (which has a corresponding token), received from account holders through the interface for provisioning a specific debit and/or credit card of Defendant (or a bank using Visa tokenization services) for use with Visa tokenization services. The server is also programmed to receive requests initiated by a cardholder customer of Defendant (or a bank using Visa tokenization services) for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder. The server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

129. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising: a first merchant identifier; a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier; the credit or debit card account holder identifier; and a designated unique account identifier selected from the at least one unique account identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message



having been received through the at least one interface and originating from the account holder's mobile device. The server is programmed to receive authorization requests initiated by an account holder for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a merchant identifier, and the account holder identifier. The server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

130. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string wherein the key string is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

131. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive a payment

request message from the merchant's payment application through the at least one interface, the payment request message comprising: a second merchant identifier; a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific authentication credential whereby the second authentication credential was received by the merchant application from the credit or debit card account holder's mobile device. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the account holder's mobile device. The server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

132. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the specific merchant by determining if: the first merchant identifier matches the second merchant identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second

transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to provide the authentication services.

133. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

134. Defendants thus infringe one or more claims of the 659 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 9 of the 659 Patent. Thus, Defendants' use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 659 Patent.

135. Defendants have directly infringed and continue to directly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.



136. Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 659 Patent by others and Defendants will continue to do so unless enjoined by this Court. Defendants' deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 659 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Defendants knew and/or were willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 659 Patent.

137. Defendants continue to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continue to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 659 Patent.

138. Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 659 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality

which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

139. Defendants have committed these acts of infringement without license or authorization.

140. By engaging in the conduct described herein, Defendants have caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Defendants are thus liable to Textile for infringement of the 659 Patent, pursuant to 35 U.S.C. § 271.

141. As a direct and proximate result of Defendants' infringement of the 659 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Defendants' past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

142. In addition, the infringing acts and practices of Defendants have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Textile is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Defendants are finally and permanently enjoined from further infringement.

143. Defendants have had actual knowledge of the 659 Patent at least as of the date when they were notified of the filing of this action. By the time of trial, Defendants will have

known and intended (since receiving such notice) that their continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 659 Patent.

144. Defendants have also indirectly and willfully infringed, and continue to indirectly and willfully infringe, the 659 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

145. Textile has been damaged as a result of the infringing conduct by Defendants alleged above. Thus, Defendants are liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

146. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 659 Patent.

#### **COUNT IV**

##### **INFRINGEMENT OF U.S. PATENT NO. 10,560,454**

147. On February 11, 2020, United States Patent No. 10,560,454 (“the 454 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

148. Textile is the owner of the 454 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 454 Patent against infringers, and to collect damages for all relevant times.

149. Regions, Capital One, Chase, and Citibank offer Visa-branded debit and/or credit cards, such as the Regions Visa Debit Card, various Regions Visa Credit Cards, the Capital One Venture X Visa Credit Card, the Capital One Venture Visa Credit Card, the Capital One Journey Visa Credit Card, the Chase Freedom Unlimited Visa Credit Card, the Chase Sapphire Preferred



Visa Credit Card, the Chase Sapphire Reserve Visa Credit Card, the Citibank Costco Anywhere Visa Credit Card, and the Citibank Costco Anywhere Visa Business Credit Card, that are used with Regions, Capital One, Chase, and/or Citibank computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client (the "Accused Instrumentality"). Visa provides services to banks for the purposes of using the Accused Instrumentality transaction-specific access authorization system. The Accused Instrumentality transaction-specific access authorization systems that are used, made, and sold by Regions, Capital One, Chase, Citibank, and Visa are implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones or computers and use those tokens, which are generated and communicated by the system, and wherein each account held by the user has its own token.


## Click to Pay with Visa

*Transfer Money and Pay*



Click to Pay with Visa<sup>1</sup> is the easy, smart and secure way to shop online with your smartphone, tablet or computer.

### It's Easy

1. Add your Regions credit card, debit card or Now Card — you only have to do this once.
2. Start shopping. When you're ready to pay, look for the Visa icon  at checkout and select the Regions card you'd like to use. You can skip guest checkout and bypass form fields.
3. Enter your user ID to complete your purchase. You won't need your password if you're shopping on a trusted device.

### It's Smart

No need to fill out credit card and shipping information every time you make a purchase. Just look for the Visa icon  at checkout to skip long forms and save time.

### It's Secure

No need to worry about identity theft or hacking. Your credit card information is stored behind multiple layers of security. Shop with confidence on any of your devices.

Sign up today to enjoy easy online checkout with fewer clicks.

(Source: <https://www.regions.com/digital-banking/transfer-money-and-pay/click-to-pay-with-visa>)



**Venture**  
**Earn 75,000 Bonus Miles**  
 once you spend \$4,000 on purchases within the first 3 months from account opening

[Card Details](#)
[Security](#)
[FAQ](#)

(Source:

[https://applynow.capitalone.com/?productId=20309&external\\_id=WWW\\_XXXXX\\_XXX\\_SEM-Brand\\_MSN\\_ZZ\\_ZZ\\_T\\_Home\\_ZZ\\_5c41d4ea-bd50-4ced-a631-97fd8a8adeef\\_86361&msclkid=af4735f015e11dab0f00566108753338](https://applynow.capitalone.com/?productId=20309&external_id=WWW_XXXXX_XXX_SEM-Brand_MSN_ZZ_ZZ_T_Home_ZZ_5c41d4ea-bd50-4ced-a631-97fd8a8adeef_86361&msclkid=af4735f015e11dab0f00566108753338))



**CHASE CREDIT CARDS** [Sign in](#)

Featured Cards | Card Finder | Card Categories | Card Brands

## Rewards Credit Cards

Find the best rewards credit card for your lifestyle, whether you're looking to earn travel rewards or get cash back rewards while shopping. Compare our rewards cards' offers and bonuses to choose the right card for you.

Chase Freedom Unlimited<sup>®</sup> credit card

★★★★★  
 (10,034 cardmember reviews)

## NEW CARDMEMBER OFFER

**\$200 bonus plus 5% grocery store offer - up to \$800 total cash back**

Earn a \$200 bonus after you spend \$500 on purchases in the first 3 months from account opening. Plus, earn 5% cash back on grocery store purchases (excluding Target<sup>®</sup> and Walmart<sup>®</sup>) on up to \$12,000 spent in the first year (that's \$600 cash back!).

## AT A GLANCE

Earn cash back for every purchase. Earn unlimited 1.5% cash back or more on all purchases, like 3% on dining and drugstores and 5% on travel purchased through Chase.

## APR

0% Intro APR for 15 months from account opening on purchases and balance transfers.<sup>‡</sup> After the intro period, a variable APR of 18.74%-27.49%.<sup>‡</sup> Balance transfer fee applies, see pricing and terms for more details.<sup>‡</sup>

## ANNUAL FEE

\$0<sup>‡</sup>

[Apply Now](#)
[Learn more >](#)

<sup>‡</sup>[Pricing & Terms](#)  
[Rewards Program Agreement \(PDF\)](#)

☐ [Compare](#) <sup>?</sup>

(Source: <https://creditcards.chase.com/rewards-credit-cards?CELL=6TKV>)





[Apply Now](#)

[\\*Pricing & Information](#)

## Costco Anywhere Visa® Card by Citi

Designed exclusively for Costco Members

### Earn 4% cash back on eligible gas and EV charging

For the first \$7,000 per year and then 1% thereafter.

A Costco membership is required to apply.

[Join Costco today.](#)

### Earn cash back on other purchases

3% cash back on restaurant and eligible travel purchases worldwide, 2% cash back on all other purchases from Costco and [Costco.com](#), 1% cash back on all other purchases.

### No Foreign Transaction Fees\*

No matter where you're traveling, when you use your Costco Anywhere Visa® Card by Citi there are no foreign transaction fees on purchases.\*

[See more details](#) ▼

Take your business to the next level



[Apply Now](#)

[\\*Pricing & Information](#)

## Costco Anywhere Visa® Business Card by Citi

Power your small business with the only business card for Costco Members

### Earn 4% cash back on eligible gas and EV charging

For the first \$7,000 per year and then 1% thereafter.

A Costco membership is required to apply.

[Join Costco today.](#)

### Earn cash back on other purchases

3% cash back on restaurant and eligible travel purchases worldwide, 2% cash back on all other purchases from Costco and [Costco.com](#), 1% cash back on all other purchases.

### No Foreign Transaction Fees\*

No matter where you're traveling, when you use your Costco Anywhere Visa® Card by Citi there are no foreign transaction fees on purchases.\*


[See more details](#) ▼

(Source:

[https://citicards.citi.com/usc/Multi/Featured/default.htm?cmp=knc|acquire|2004|FCP|CARDS|UNK|MSN|BR&gclid=3d98efa69e8110b186bd8c37bc1d66e3&gclsrc=3p.ds&msclkid=3d98efa69e8110b186bd8c37bc1d66e3&BT\\_TX=1&tab=all-cards](https://citicards.citi.com/usc/Multi/Featured/default.htm?cmp=knc|acquire|2004|FCP|CARDS|UNK|MSN|BR&gclid=3d98efa69e8110b186bd8c37bc1d66e3&gclsrc=3p.ds&msclkid=3d98efa69e8110b186bd8c37bc1d66e3&BT_TX=1&tab=all-cards))

### 3 Core digital payment tokenization programs


There are three programs to choose from. Each program is described below and available on your dashboard after you create an account. You can apply to one or more based on your certification needs.



**Tokenization eCommerce and Card on File (card not present)**

Online payments continue to suffer worse authorization rates compared to in-store. By eliminating PAN storage and transfer, Visa Tokens help reduce data breach, mitigate fraud and create a trusted environment which can improve authorization rates for digital transactions.


[Apply Now](#)



**Click to Pay (Visa Secure Remote Commerce)**

Click to Pay was designed to deliver a fast, easy, and secure digital guest checkout experience by eliminating passwords and tedious form fill. By making the payment experience more streamlined and consistent across digital channels, we look to reduce cart abandonment and drive higher conversion.

[Apply Now](#)



**Tokenization - TSP (card present)**

Whether it's a mobile phone or other payment-enabled devices, Visa's Tokens enable payments to be made with the wave of a hand. We're partnering with mobile wallets, device manufacturers, and platform providers to create a convenient, secure, and touch-free way to pay at point-of-sale.

[Apply Now](#)

(Source: <https://partner.visa.com/site/programs/visa-ready/digital-payments.html>)

## All you need to know about Tokenization

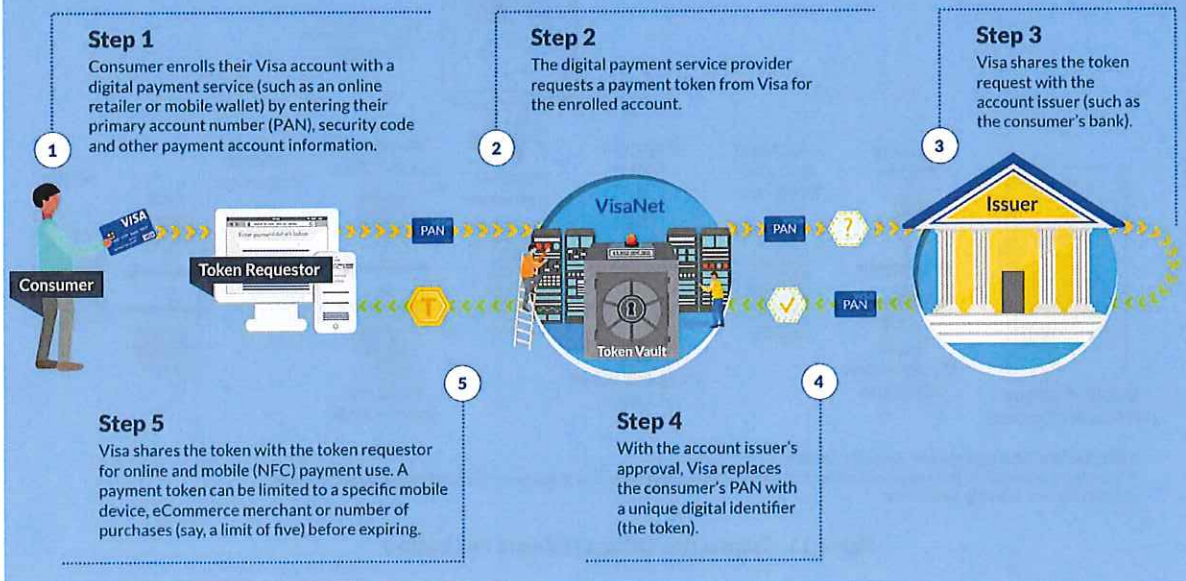
Visa Token Service, a new security technology from Visa, replaces sensitive account information, such as the 16-digit account number, with a unique digital identifier called a *token*. The token allows payments to be processed without exposing actual account details that could potentially be compromised.



(Source: <https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf>)

## How Visa Token Service Works

The Visa Token Service enables digital payment service providers and financial institutions to offer their customers a safe way to shop online and with mobile devices. Here's how a token is initiated.

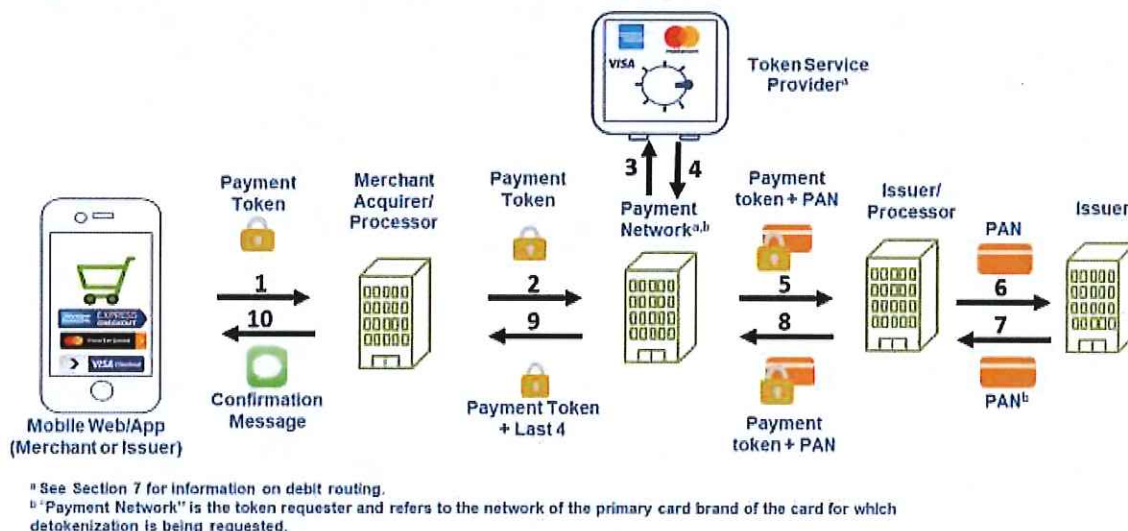


(Source: <https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf>)



### 5.3 Transaction Processing (Network Pay Button)

Figure 11 illustrates the processing for tokenized transactions using a mobile phone with a network pay button. Note that not all transactions with pay buttons will be tokenized.



**Figure 11. Transaction Using a Network Pay Button**

During the transaction process, the following steps occur:

1. The cardholder uses a mobile app or web browser interface at checkout and selects to pay using a cloud-based wallet. The cardholder is redirected to the cloud wallet server for authentication. The cardholder verifies the amount and selects the token for payment. The cardholder is redirected to the mobile application or web with a payment transaction identifier.<sup>7</sup> The payment transaction identifier is passed to merchant's back office to complete the payment

<sup>7</sup> The payment transaction identifier is a unique number identifying a transaction the customer has accepted on the cloud wallet server. It does not include a token or cryptogram data.

process. The merchant's back office uses the payment transaction identifier to obtain a token and cryptogram from the cloud wallet server. The merchant's back office sends the token and cryptogram to the merchant acquirer/processor.

2. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that this transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to a clear PAN.
4. The TSP verifies the cryptogram and returns the clear PAN to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor sends the transaction response to the mobile application. The merchant's back office confirms payment status to the cloud wallet server.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

150. The Accused Instrumentality includes a computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client. For example, an account holder of Defendant (or an account holder of a bank using Visa tokenization services) requests Defendant to provision a specific debit and/or credit card for use with Visa tokenization services. The account holder can then request for payment to be made by Defendant (or a bank using Visa tokenization services) to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder using his or her Visa tokenization information. In initiating the request, the account holder's

smartphone, mobile app, or web browser receives certain transaction specific information from the merchant, which is incorporated into a cryptogram generated by a server that is transmitted to the merchant, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted to the merchant. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

151. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a user's application, a service client's application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with an account holder's mobile device, a merchant's payment application, server, and/or other software or hardware, or both. The interface is also programmed to receive requests initiated by a cardholder customer of Defendant (or a bank using Visa tokenization services) for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder. This interface is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

152. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration information received from the user through the at least one interface, the registration information comprising a user identifier and at least one secured resource identifier associated with the common identifier of the secured resource, wherein the common identifier and secured resource



identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card, the debit and/or credit card account number (which has a corresponding token), and the CVV number received from account holders through the interface for provisioning a specific debit and/or credit card of Defendant (or a bank using Visa tokenization services) for use with Visa tokenization services. The server is also programmed to receive requests initiated by a cardholder customer of Defendant (or a bank using Visa tokenization services) for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder. The server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

153. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the secured resource by the service client, the authorization request message having been received through the at least one interface from the user's application and comprising: a first service client identifier; a first transaction specific information; the user identifier; and a designated secured resource identifier selected from one of the at least one secured resource identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the account holder's mobile device. The server is programmed to receive authorization requests initiated by account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a CVV number, a merchant

identifier, other token information, and the account holder identifier. The server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

154. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string and does not include or reveal the common identifier associated with the designated secured resource identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

155. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive an access request message from the service client's application through the at least one interface, the payment request message comprising: a second service client identifier; a second transaction specific information; and a second transaction specific authentication credential whereby the second transaction specific authentication credential was received by the service client's

application from the user's application. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the account holder's mobile device. The server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to receive the messages.

156. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the user's request to access the secured resource associated with the designated secured resource identifier without transmitting or otherwise providing the common identifier of the secured resource to the service client by determining if: the first service client identifier matches the second service client identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Defendants or through an agent with whom Defendants have contracted to provide the authentication services.



157. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

158. Defendants thus infringe one or more claims of the 454 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 8 of the 454 Patent. Thus, Defendants' use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 454 Patent.

159. Defendants have directly infringed and continue to directly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

160. Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 454 Patent by others and Defendants will continue to do so unless enjoined by this Court. Defendants' deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make

available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 454 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Defendants knew and/or were willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 454 Patent.

161. Defendants continue to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continue to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 454 Patent.

162. Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 454 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

163. Defendants have committed these acts of infringement without license or authorization.

164. By engaging in the conduct described herein, Defendants have caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Defendants are thus liable to Textile for infringement of the 454 Patent, pursuant to 35 U.S.C. § 271.

165. As a direct and proximate result of Defendants' infringement of the 454 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Defendants' past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

166. In addition, the infringing acts and practices of Defendants have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Textile is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Defendants are finally and permanently enjoined from further infringement.

167. Defendants have had actual knowledge of the 454 Patent at least as of the date when they were notified of the filing of this action. By the time of trial, Defendants will have known and intended (since receiving such notice) that their continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 454 Patent.

168. Defendants have also indirectly and willfully infringed, and continue to indirectly and willfully infringe, the 454 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

169. Textile has been damaged as a result of the infringing conduct by Defendants alleged above. Thus, Defendants are liable to Textile in an amount that adequately compensates



it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

170. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 454 Patent.

**ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT**

171. Defendants have also indirectly infringed the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent by inducing others to directly infringe the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent. Defendants have induced the end-users, Defendants' customers, to directly infringe (literally and/or under the doctrine of equivalents) the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent by using the Accused Instrumentality.

172. Defendants took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

173. Such steps by Defendants included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner; advertising and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

174. Defendants has performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent and

with the knowledge that the induced acts constitute infringement, at least since the filing of the Complaint.

175. Defendants were and are aware that the normal and customary use of the Accused Instrumentality by Defendants' customers would infringe the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent. Defendants' inducement is ongoing.

176. Defendants direct or control the use of the Accused Instrumentality nationwide through their own websites, servers, and in their own branches, including in Texas and elsewhere in the United States, and expects and intends that the Accused Instrumentality will be so used.

177. Defendants took active steps, directly and/or through contractual relationships with others, with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

178. Defendants performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts would constitute infringement.

179. Defendants' inducement is ongoing.

180. Defendants have also indirectly infringed by contributing to the infringement of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent. Defendants have contributed to the direct infringement of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent by the end-user of the Accused Instrumentality.

181. The Accused Instrumentality has special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the 079

Patent, the 802 Patent, the 659 Patent, and the 454 Patent, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

182. As described above, the special features include securely authorizing specific transactions without providing a credit or debit card number to the merchant used in a manner that infringes the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent.

183. The special features constitute a material part of the invention of one or more of the claims of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

184. Defendants' contributory infringement is ongoing.

185. Defendants have had knowledge of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent at least since the filing of the Complaint.

186. Defendants' customers have infringed the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent.

187. Defendants encouraged their customers' infringement.

188. Defendants' direct and indirect infringement of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Textile' rights under the patents.

189. Textile has been damaged as a result of the infringing conduct by Defendants alleged above. Thus, Defendants are liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

**JURY DEMAND**



Textile hereby requests a trial by jury on all issues so triable by right.

**PRAYER FOR RELIEF**

Textile requests that the Court find in its favor and against Defendants, and that the Court grant Textile the following relief:

- a. Judgment that one or more claims of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Defendants and/or all others acting in concert therewith;
- b. A permanent injunction enjoining Defendants and their officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent by such entities;
- c. Judgment that Defendants account for and pay to Textile all damages to and costs incurred by Textile because of Defendants' infringing activities and other conduct complained of herein, including an award of all increased damages to which Textile is entitled under 35 U.S.C. § 284;
- d. That Textile be granted pre-judgment and post-judgment interest on the damages caused by Defendants' infringing activities and other conduct complained of herein;
- e. That this Court declare this an exceptional case and award Textile its reasonable attorney's fees and costs in accordance with 35 U.S.C. § 285; and
- f. That Textile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: January 9, 2023

Respectfully submitted,



Matthew J. Antonelli

Texas Bar No. 24068432

matt@ahtlawfirm.com

Zachariah S. Harrington

Texas Bar No. 24057886

zac@ahtlawfirm.com

Larry D. Thompson, Jr.

Texas Bar No. 24051428

larry@ahtlawfirm.com

Christopher Ryan Pinckney

Texas Bar No. 24067819

ryan@ahtlawfirm.com

ANTONELLI, HARRINGTON

& THOMPSON LLP

4306 Yoakum Blvd., Ste. 450

Houston, TX 77006

(713) 581-3000

Stafford Davis

State Bar No. 24054605

sdavis@stafforddavisfirm.com

Catherine Bartles

Texas Bar No. 24104849

cbartles@stafforddavisfirm.com

THE STAFFORD DAVIS FIRM

815 South Broadway Avenue

Tyler, Texas 75701

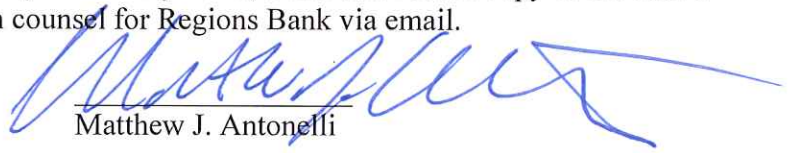
(903) 593-7000

(903) 705-7369 fax

*Attorneys for Textile Computer Systems, Inc.*

**CERTIFICATE OF SERVICE**

I hereby certify that on the 9th day of January 2023, a true and correct copy of the above and foregoing document was served on counsel for Regions Bank via email.



Matthew J. Antonelli